Hamlet

Wi-Fi Personal Bridge 150

AP Router Portatile Wireless

Manuale Utente

HNW150APBR

www.hamletcom.com

Indice del contenuto

1 Introduzione 8

Caratteristiche 8

Requisiti dell'apparato 8

Utilizzo del presente documento 9

Convenzioni di notazione 9

Convenzioni tipografiche 9

Messaggi speciali 9

2 Iniziare a conoscere l'apparato 10

Requisiti del Computer / Sistema 10

Contenuto dell'imballo 10

Significato degli indicatori LED 10

Lato superiore 10

Pannello posteriore, pannello laterale sinistro e lato inferiore 11

3 Configurazione del computer per ottenere l'indirizzo IP in automatico, per differenti Sistemi Operativi 13

Windows 98SE / ME / 2000 / XP 13

Windows Vista-32/64 15

Windows 7-32/64 18

4 Collegamenti dell'apparato 21

Collegamento dell'apparato 21

Modalità Router (l'interfaccia WAN è connessa ad Internet mediante una connessione xDSL o un Modem di linea): 22

Modalità Client (l'interfaccia WAN è connessa mediante un Router WLAN, xDSL o Modem di linea ad Internet): 23

Modalità WiFi-AP (l'interfaccia WAN è connessa alla WAN, la porta LAN o l'interfaccia WLAN è connessa mediante Router WLAN, xDSL o Modem di Linea ad Internet): 24

Modalità WiFi-AP (l'interfaccia WAN è connessa alla WAN, la porta LAN o l'interfaccia WLAN è connessa mediante Router WLAN, xDSL o Modem di linea ad Internet): 25

5 CD Utility 26

Configurazione avanzata per la modalità Router 26

Configurazione avanzata in modalità Client 31

Configurazione avanzata per la modalità WiFi-AP Mode 1 37

Configurazione avanzata per la modalità WiFi-AP Mode 2 - Universal Repeater (il Router opera come AP e Client contemporaneamente) 42

Configurazione avanzata per la modalità WiFi-AP Mode 3 - WDS 47

Configurazione avanzata per la modalità WiFi-AP Mode 3 – WDS + AP 51

Connessione Wireless (solo per la modalità Router) 55

6 Conoscere il tipo di accesso Internet/WAN disponibile 57

Accesso Internet/WAN di tipo Client DHCP 58

Accesso Internet/WAN di tipo IP statico 58

Accesso Internet/WAN di tipo Client PPPoE 60

7 Come utilizzare le pagine WEB 61

Accesso alle pagine Web 61

Verifica della configurazione 63

Configurazione di default del dispositivo 63

8 Setup rapido (la funzione può variare in funzione della modalità Router, Client o WiFi-AP) 65

Configurazione della modalità operativa 66

Gateway 66

Wireless ISP 67

Configurazione della Interfaccia WAN 68

Static IP 69

DHCP Client 70

PPPoE 71

PPTP 72

L2TP 73

Configurazione di base della rete Wireless 74

AP (Access Point) 75

Client 76

WDS (Wireless Distribution System) 77

Solo WDS (Wireless Distribution System) 79

AP (Access Point) + WDS (Wireless Distribution System) 80

Configurazione Wireless Security 81

Configurare la tecnica WEP 64bit ASCII (5 caratteri) 83

Configurare la tecnica WEP 64bit HexI (10 caratteri) 84

Configurare la tecnica WEP 128bit ASCII (13 caratteri) 85

Configurare la tecnica WEP 128bit Hex (26 caratteri) 86

Configurare la tecnica WPA (AES) Hex (64 caratteri) 88

Configurare la tecnica WPA (AES) HEX (64 caratteri) 90

Configurare la tecnica WPA2 (Mixed) Passphrase 91

Configurare la tecnica WPA2 (Mixed) HEX (64 caratteri) 92

9 Rete Wireless 93

Configurazioni di base 93

Configurazioni avanzate 95

Sicurezza 96

WEP + Encryption Key 98

WEP + Use 802.1x Authentication 99

WPA/WPA2/WPA2 Mixed + Personal (Pre-Shared Key) 100
WPA/WPA2/WPA2 Mixed + Enterprise (RADIUS) 101
Controllo Accessi 103
Allow Listed 103
Deny Listed 105
Configurazione WDS 106
Configure WDS (Wireless Distribution System) only 107
Configurazione AP (Access Point) + WDS (Wireless Distribution System) 111
Site Survey (sorveglianza di sito) 115
Configurazione Wireless ISP + Wireless client + Site Survey 116
WPS 120
Introduzione al sistema WPS 121
Caratteristiche WPS supportate 121
Modalità AP 122
AP come Enrollee 122
AP come Registrar 122
AP come Proxy 122
Modalità Infrastructure-Client 122
Istruzioni sull'impiego come AP e come Client 122
Pagina Wireless Advanced Settings 123
Impiego dell' AP come enrollee 124
Impiego dell' AP come registrar 133
Modalità AP 133
Metodo Push Button 136
Scheduling della rete Wireless 139

10 Interfaccia LAN 140

Setup della interfaccia LAN 140
Cambio Indirizzo IP e Subnet Mask della LAN 142
Show Client 145

11 Interfaccia WAN 146

Configurazione della connessione con IP statico 150
Configurazione della connessione DHCP Client 151
Configurazione della connessione mediante PPPoE 152
Configurazione della connessione mediante PPTP 153
Configurazione della connessione mediante L2TP 155
Duplicazione del MAC Address 157

12 Filtri associati alle porte 159

Filtro per la porta 80 - protocollo TCP 160
Filtro per la porta 53 protocollo UDP 161

13 Filtri associati all'indirizzo IP 162
Filtri IP per protocollo TCP con indirizzo IP specifico 163
Filtri IP per protocollo UDP con indirizzo IP 165
Filtri IP per entrambi i protocolli TCP e UDP con indirizzo IP specifico 167
14 Filtri associate al MAC Address 169
Filtri associate a specifici MAC Address 170
15 Reindirizzamento porte 172
Reindirizzamento porte per protocollo TCP con specifico indirizzo IP....173
Reindirizzamento porte per protocollo UDP con specifico indirizzo IP 174
16 Filtri associati all'indirizzo URL 175
Filtri associati a specifici URL 175
17 DMZ 177
Indirizzo IP dell'Host DMZ....177
18 VLAN 179
19 QoS 180
20 Route Setup 181
21 Stato del dispositivo 182
22 Statistiche 183
23 DNS Dinamico 184
Configurare DynDNS 186
Configurazione TZO....187
24 Configurazione Time Zone 188
Configurazione del Server SNTP e del Client SNTP....188
25 Denial-of-Service 190
Denial-of-Service....190
26 Log 192
Log di sistema 192
27 Aggiornamento Firmware 194
Informazioni utili circa la versione firmware....194
Aggiornamento manuale del firmware 194
28 Salvataggio/Lettura della configurazione 196
Salvataggio della configurazione in un file 196
Lettura della configurazione da un file....198
Ripristino dei valori di default 200
29 Password 202
Configurazione di Username e Password....202
30 Logout 204

Logout....204
A Configurazione dei Computer 205
Configurazione della connessione Ethernet sul PC....205
Prima di iniziare....205
Windows® XP....205
Windows 2000....205
Windows Me....206
Windows 95, 98....207
Assegnazione statica degli indirizzi IP sui computer....207
B Indirizzi IP, Network e Subnet Mask 209
Indirizzi IP....209
Struttura di un indirizzo IP....209
Classi di reti....209
Subnet mask....210
C UPnP Control Point Software su Windows ME/XP 212
UPnP Control Point Software su Windows ME....212
UPnP Control Point Software su Windows XP con Firewall....212
Requisiti SSDP....213
D Risoluzione dei problemi 215
Suggerimenti per la soluzione dei problemi....215
Diagnostica mediante le utility IP....217
ping....217
nslookup....217
E Glossario 219

Gentile Cliente,
La ringraziamo per la fiducia riposta nei nostri prodotti. La preghiamo di seguire le norme d'uso e manutenzione che seguono. Al termine del funzionamento di questo prodotto La preghiamo di non smaltirlo tra i rifiuti urbani misti, ma di effettuare per detti rifiuti una raccolta separata negli appositi raccoglitori di materiale elettrico/elettronico o di riportare il prodotto dal rivenditore che lo ritirerà gratuitamente.

Dichiarazione di responsabilità
L'importatore per l'Europa dichiara che il prodotto è conforme alle normative CE. I riferimenti all'importatore e le modalità di contatto sono disponibili nella sezione "Chi siamo" del sito web www.hamletcom.com.

L'importatore per L'Italia è:
Careca Italia S.p.A.
Partita IVA numero 02078660350
www.careca.com

La dichiarazione di conformità CE completa e tutta la documentazione relativa al prodotto è disponibile contattando Hamlet all'indirizzo info@hamletcom.com specificando codice del prodotto e tipo documentazione richiesta.

Informiamo che il prodotto è stato realizzato con materiali e componenti in conformità a quanto previsto dalle direttive RoHS: 2002/95/CE, RAEE: 2003/96/CE, D.Lgs. 151/2005 e le direttive CE secondo i seguenti standard: EN 300 328 V1.7.1 05-2006, EN 301 489-1 V1.8.1 04-2008, EN 301 489-17 V2.1.1 05-2009, EN 300 386 V1.5.1 10-2010, EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011.

CE Mark Warning
Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

Marchi commerciali
Tutti i marchi e i nomi di società citati in questa guida sono utilizzati al solo scopo descrittivo e appartengono ai rispettivi proprietari.

Variazioni
La presente guida ha scopo puramente informativo e può essere modificata senza preavviso. Sebbene questo documento sia stato compilato con la massima accuratezza, Hamlet non si assume alcuna responsabilità per eventuali errori od omissioni e all'uso delle informazioni in esso contenute. Hamlet si riserva il diritto di modificare o aggiornare il prodotto e la guida senza alcuna limitazione e senza obbligo di preavviso.

1 Introduzione

Complimenti per l'acquisto del Router AP. Tale dispositivo consente di realizzare un accesso ad Internet per mezzo di una connessione alta velocità di tipo xDSL o Modem di linea.

Il presente manuale descrive le procedure per collegare il Router AP e per configurarlo opportunamente così da ottenere le migliori prestazioni.

Caratteristiche

Di seguito solo elencate le principali caratteristiche del dispositivo, utili per chi già possiede conoscenze dei protocolli di rete. Per gli utenti meno esperti, i successivi capitoli di questa guida forniscono informazioni sufficienti ad utilizzare al meglio il Router AP.

Le principali caratteristiche possono essere sintetizzate in:

- Router Ethernet 10/100Base-T per permettere la connessione ad Internet a tutti i computer della propria rete LAN
- Funzioni NAT (Network Address Translation) per la sicurezza della rete LAN
- Configurazione di rete mediante Server DHCP e Client DHCP
- Servizi di routing IP, di configurazione DNS, servizi di RIP e servizi IP
- Supporto remoto per aggiornamento software
- Programma di configurazione di facile utilizzo di tipo WEB (accesso al programma mediante browser Web)

Il Modem integra uno Switch Ethernet interno per consentire la connessione diretta ad una rete Ethernet 10/100BASE-T, mediante interfaccia RJ-45, permettendo al contempo il collegamento diretto di un PC o di un altro dispositivo Ethernet.

Requisiti dell'apparato

Allo scopo di utilizzare il Router AP è necessario disporre di:

- una connessione Internet a Banda larga RJ-45 mediante modem xDSL o modem di linea,
- le informazioni di configurazione fornite dal provider ISP (Internet Service Provider) circa il tipo di connessione Internet disponibile e gli indirizzi necessari per configurare l'accesso ad Internet,
- uno o più computer, ciascuno dotato di interfaccia Ethernet (Scheda di rete 10Base-T/100Base-T),
- Protocollo TCP/IP attivo su ciascun PC,
- Web browser, per la configurazione del sistema. I browser supportati sono ad esempio Internet Explorer 4 o Netscape 4 o versioni superiori. Si noti che la versione 4 di ciascun browser è la versione minima utilizzabile – per una visualizzazione ottimale dei dati di configurazione, si consiglia di utilizzare Internet Explorer 5 o Netscape 6.1

Nota

Non è necessario utilizzare un hub o uno switch per collegare più PC al Router AP in rete LAN Ethernet. Infatti, il Router consente di collegare fino a 4 PC direttamente alle porte Ethernet, presenti sul pannello posteriore.

Utilizzo del presente documento

Convenzioni di notazione

- Gli acronimi utilizzati sono normalmente definiti la prima volta che vengono utilizzati e comunque riportati nel glossario in fondo alla presente guida.
- Per brevità, il Router AP è denominato nelle successive descrizioni anche come “l’apparato” o "il dispositivo".
- Il termine *LAN* identifica un gruppo di computer collegati in rete Ethernet e localizzati nello stesso sito.

Convenzioni tipografiche

- Il *testo in italico* è utilizzato per identificare voci di menù o elementi di liste di selezione oppure per i nomi delle pagine Web visualizzate.
- Il **testo in grassetto** è utilizzato per indicare termini o frasi (stringhe di caratteri) da digitare nei campi del programma oppure per enfatizzare punti importanti nel discorso.

Messaggi speciali

Il presente manuale utilizza le seguenti notazioni grafiche per mettere in evidenza specifiche istruzioni o descrizioni.

Nota

Fornisce spiegazioni o informazioni ritenute importanti (benché non essenziali) circa l'argomento che si sta descrivendo.

Definizione

Dettaglia termini o acronimi che potrebbero non essere familiari alla maggior parte degli utenti. Tali termini sono comunque inclusi nel Glossario.

ATTENZIONE

Mette in evidenza informazioni importanti ed essenziali, includendo informazioni necessarie per la sicurezza del personale o dell'integrità del sistema.

2 Iniziare a conoscere l'apparato

Requisiti del Computer / Sistema

- Processore Pentium 200MHz o superiore
- Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows Vista o Windows 7
- RAM 64MB o superiore
- 25MB di spazio libero su disco

Contenuto dell'imballo

- Router 802.11n Pocket AP
- CD-ROM (Software e Manuale)
- Guida rapida all'installazione
- Cavo Ethernet (RJ-45)
- Adattatore di alimentazione

Significato degli indicatori LED

Lato superiore

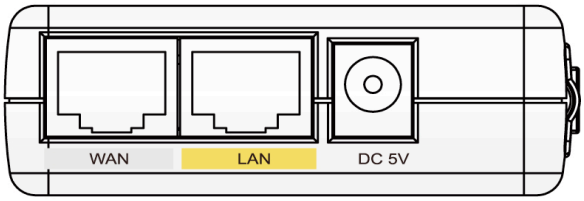
Sul lato superiore sono presenti gli indicatori LED (Light Emitting Diodes) necessari a visualizzare lo stato operativo dell'apparato.

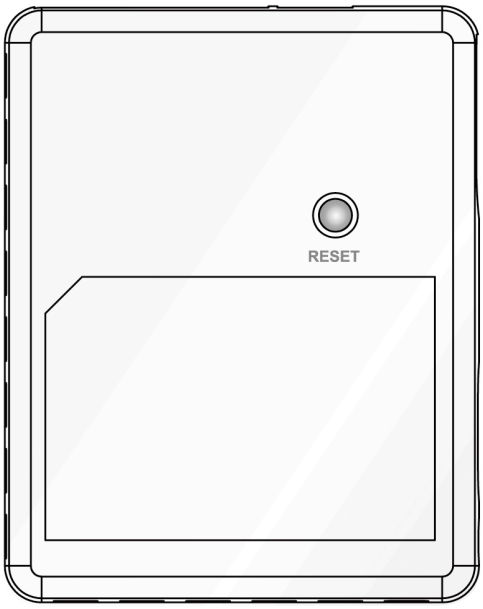
Indicazione	Colore	Funzione
POWER	verde	ON: il dispositivo è alimentato OFF: il dispositivo è spento

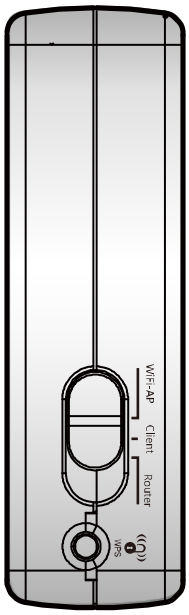
Internet	verde	ON: collegamento WAN attivo OFF: assenza del collegamento WAN Lampeggio: scambio dati con rete Internet
WLAN	verde	ON: collegamento WLAN attivo Lampeggio: scambio dati con rete Wireless
WPS	verde	OFF: collegamento WPS non attivo Lampeggio: scambio dati con WPS
LAN	verde	ON: collegamento LAN attivo OFF: assenza del collegamento LAN Lampeggio: scambio dati con rete LAN

Pannello posteriore, pannello laterale sinistro e lato inferiore

Sul pannello posteriore, sul pannello laterale e sul lato inferiore dell'apparato sono presenti: un pulsante di Reset (per il ripristino dei valori di default), le porte per i collegamenti alle reti ed il connettore per l'alimentazione elettrica.







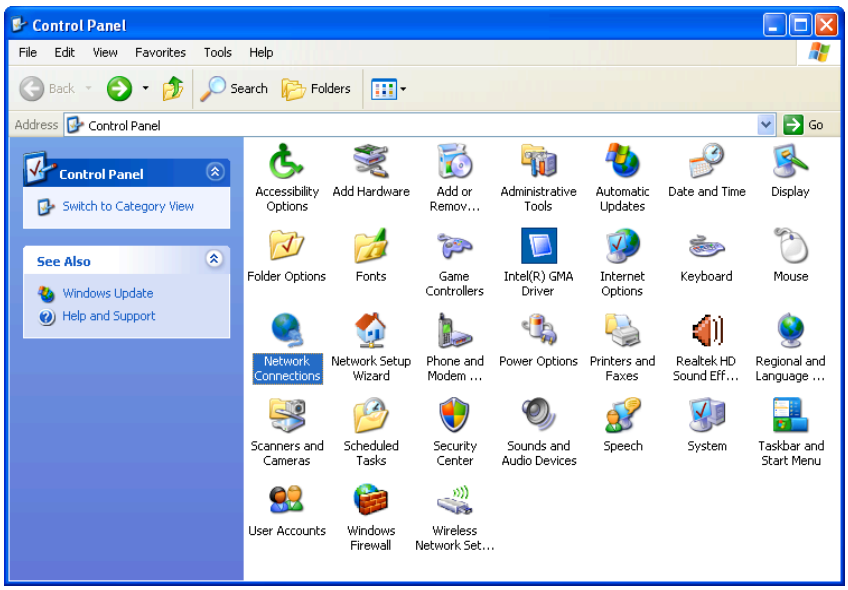
Indicazione	Funzione
DC 5V	Connettore per l'adattatore di rete
LAN	Connettore per rete LAN, mediante la quale collegare l'apparato ad un PC
WAN	Connettore per rete WAN xDSL o Modem di linea
WPS	Pulsante per l'attivazione delle funzionalità WPS. Premendo il pulsante per almeno 3 secondi, il LED WPS lampeggia per indicare l'avvio della modalità WPS. Dopo aver premuto il pulsante, premere il corrispettivo pulsante WPS sull'adattatore wireless o sul dispositivo WPS da associare. L'operazione deve essere eseguita entro 120 secondi (2 minuti) da quando si è premuto il pulsante WPS sul Router.
Commutatore	Commutatore per impostare il Router AP in modalità Router, Client o WiFi-AP
RESET	Pulsante di Reset. Effettua il **RESET** del router 802.11n Pocket AP ripristinando la configurazione di default (configurazione di fabbrica). Premendo il pulsante per almeno 6 secondi si avvia il **RESET** del dispositivo e la configurazione di default viene automaticamente ripristinata.

3 Configurazione del computer per ottenere l'indirizzo IP in automatico, per differenti Sistemi Operativi

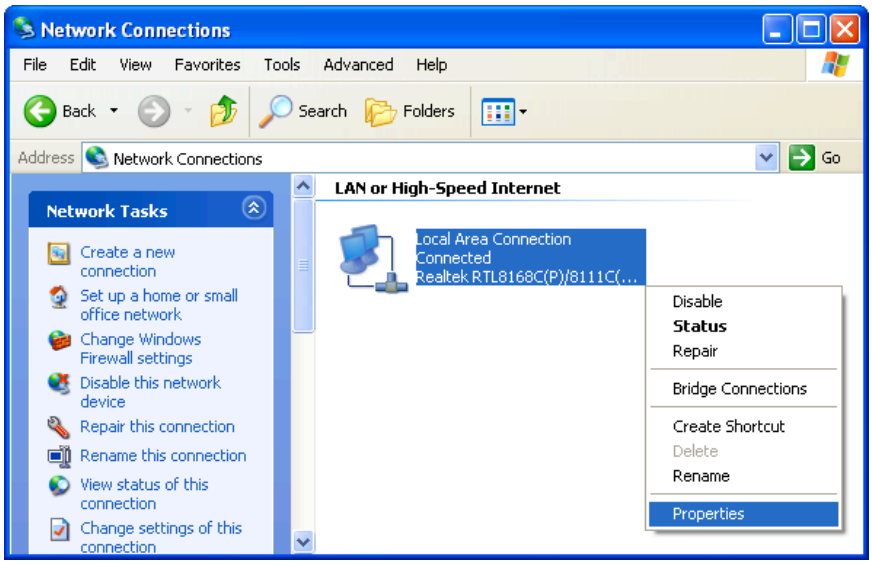
Prima di avviare la configurazione del Router 802.11n Pocket AP, è necessario configurare il PC come descritto di seguito, per ottenere l'indirizzo IP ed il server DNS automaticamente.

Windows 98SE / ME / 2000 / XP

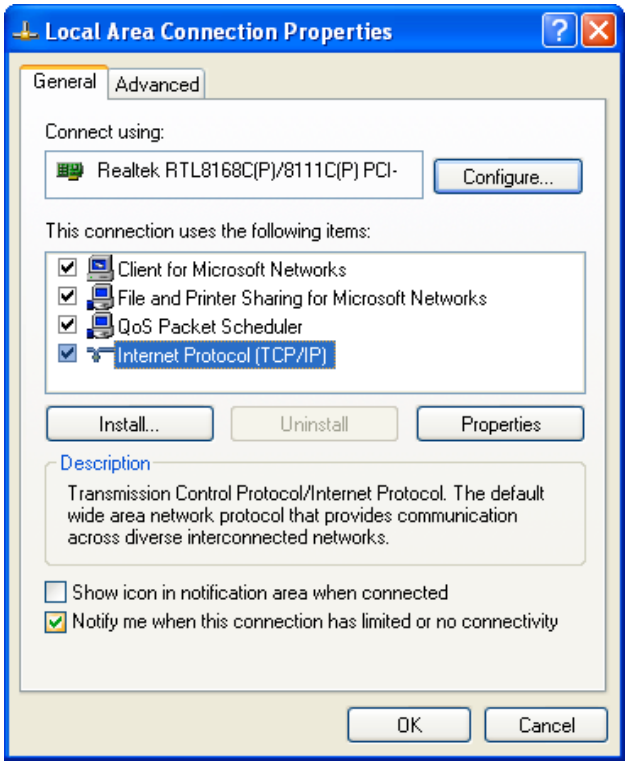
1. Fare click su "**Start**" -> "**Control Panel**" (in visualizzazione classica). Nella finestra del Pannello di Controllo, fare doppio click su "**Network Connections**" per proseguire.



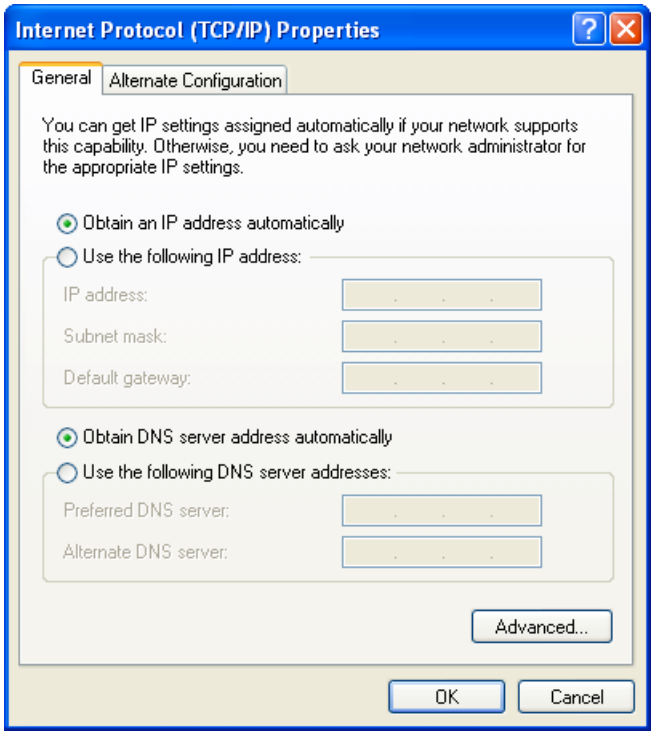
2. Selezionare con il tasto destro del mouse la voce "**Local Area connection**" e quindi selezionare "**Properties**" dal menù.



3. Fare doppio click su "**Internet Protocol (TCP/IP)**".



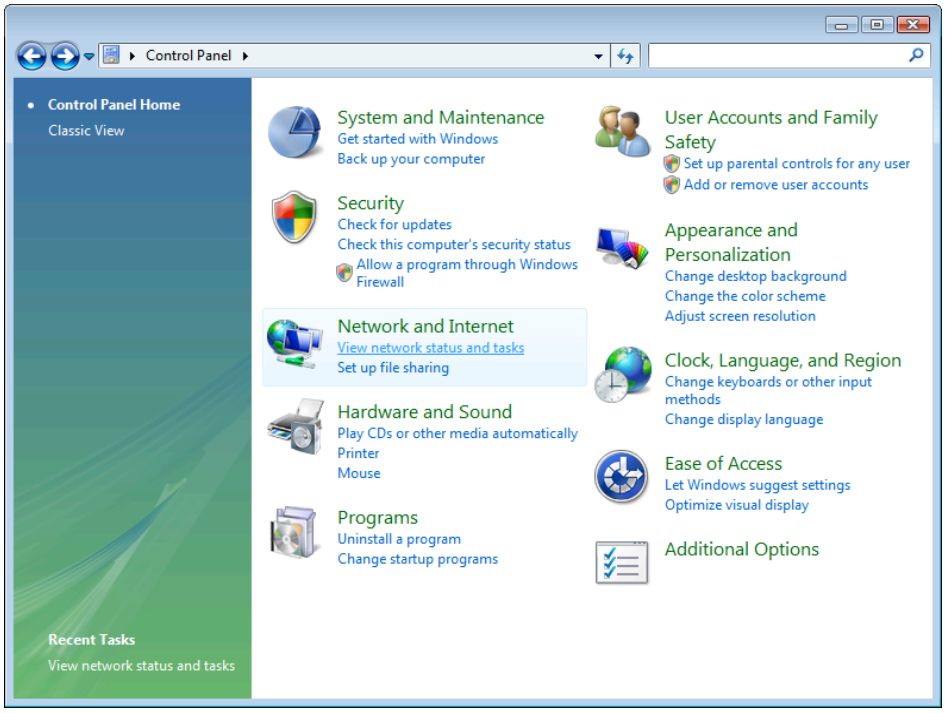
4. Selezionare "**Obtain an IP address automatically**" e "**Obtain DNS server address automatically**" e quindi premere "**OK**" per proseguire.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

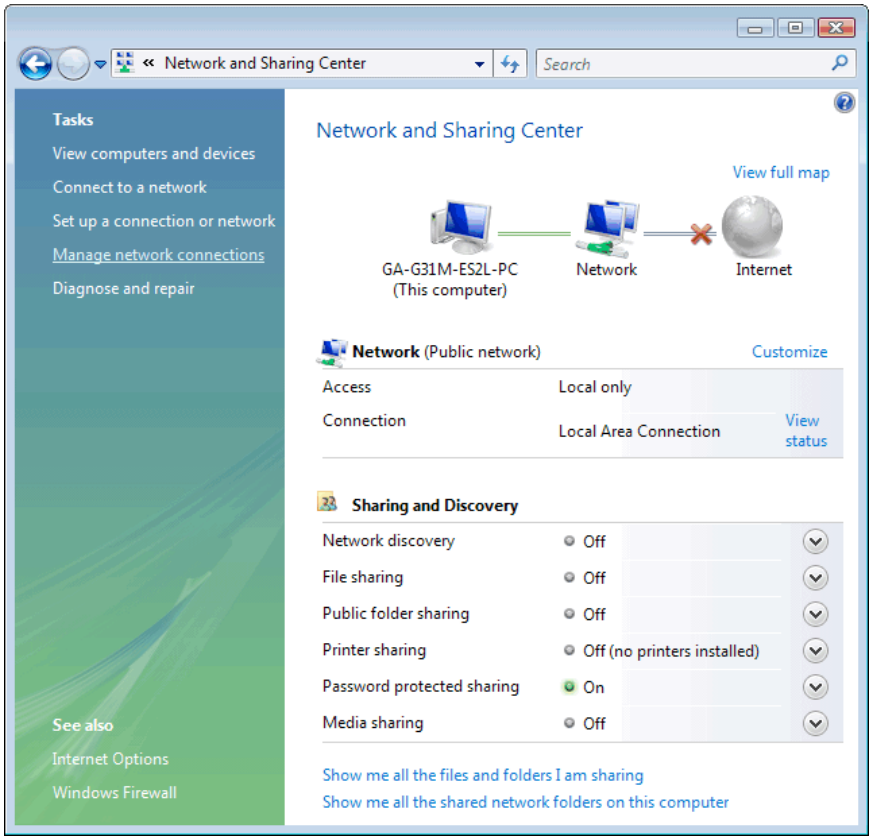
5. Selezionare "**Show icon in notification area when connected**" (si veda la schermata al punto 3) per visualizzare una icona nella area delle notifiche quando si è instaurata la connessione e premere "**OK**" per completare la procedura.

Windows Vista-32/64

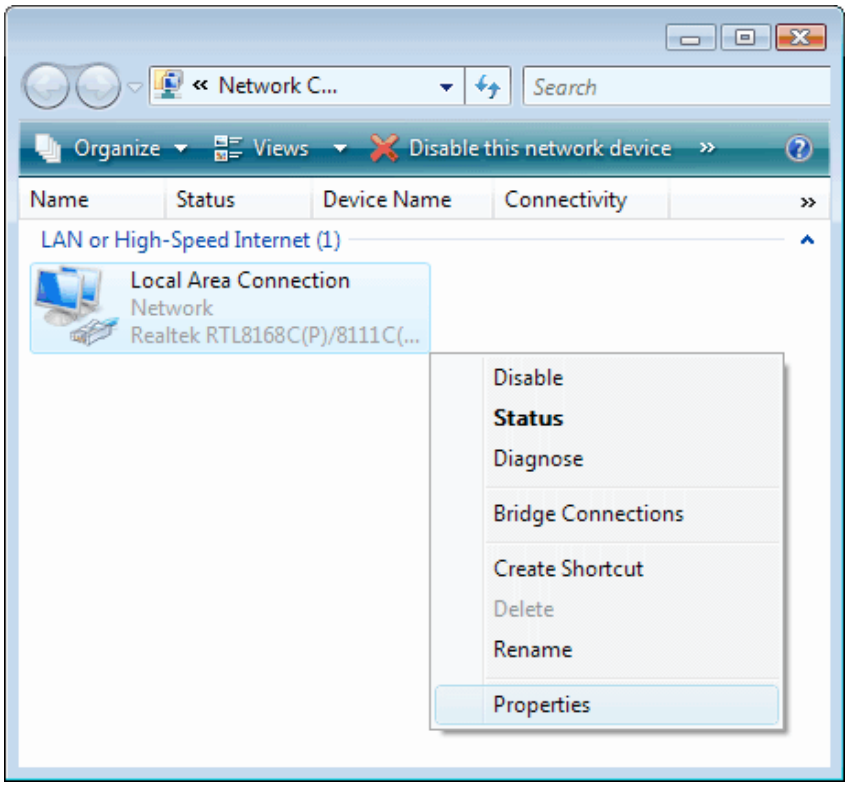
1. Fare click su “**Start**” -> “**Control Panel**” -> “**View network status and tasks**”.



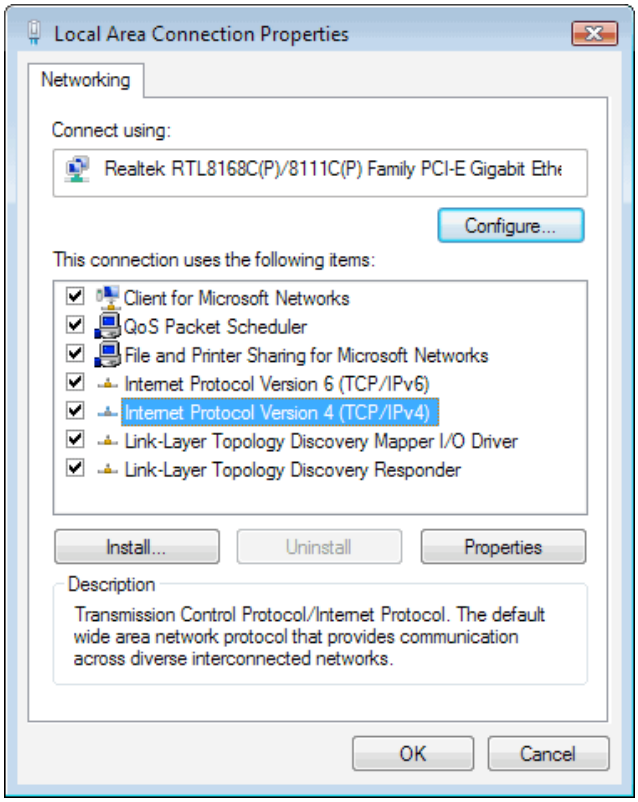
2. Nella finestra di gestione delle connessioni di rete, fare click su “**Manage network connections**” per proseguire.



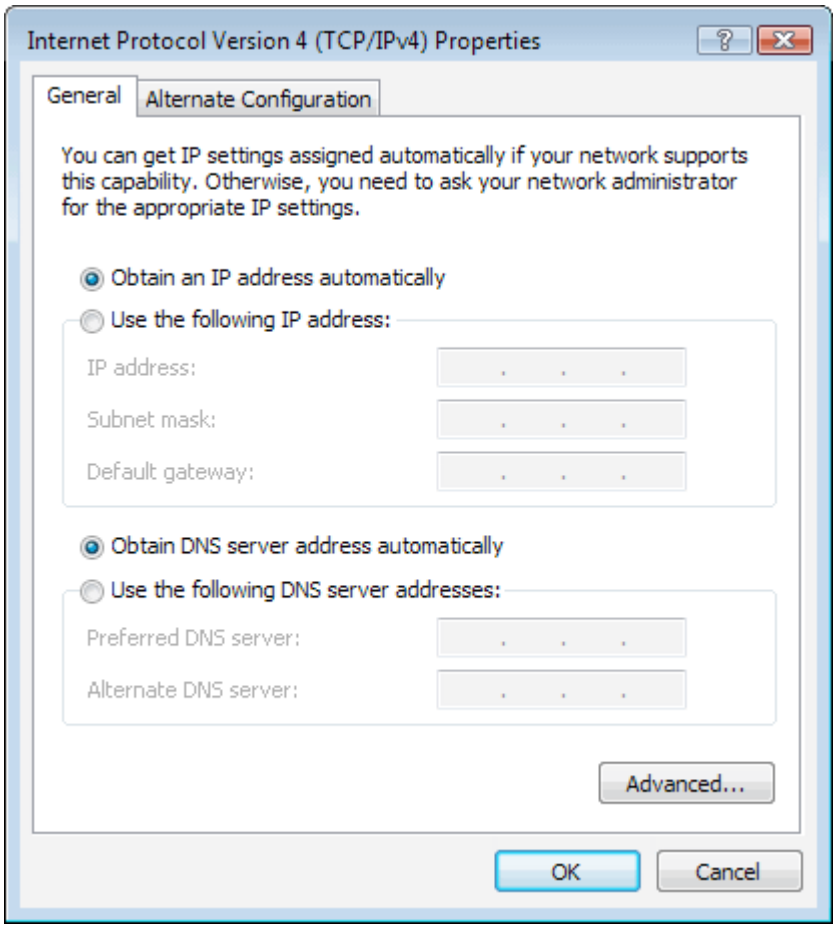
3. Selezionare con il tasto destro del mouse la voce "**Local Area connection**" e quindi selezionare "**Properties**" dal menù.



4. Verrà visualizzata la schermata " **User Account Control**" e quindi premere "**Continue**" per proseguire.
5. Fare doppio click su "**Internet Protocol Version 4 (TCP/IPv4)**".



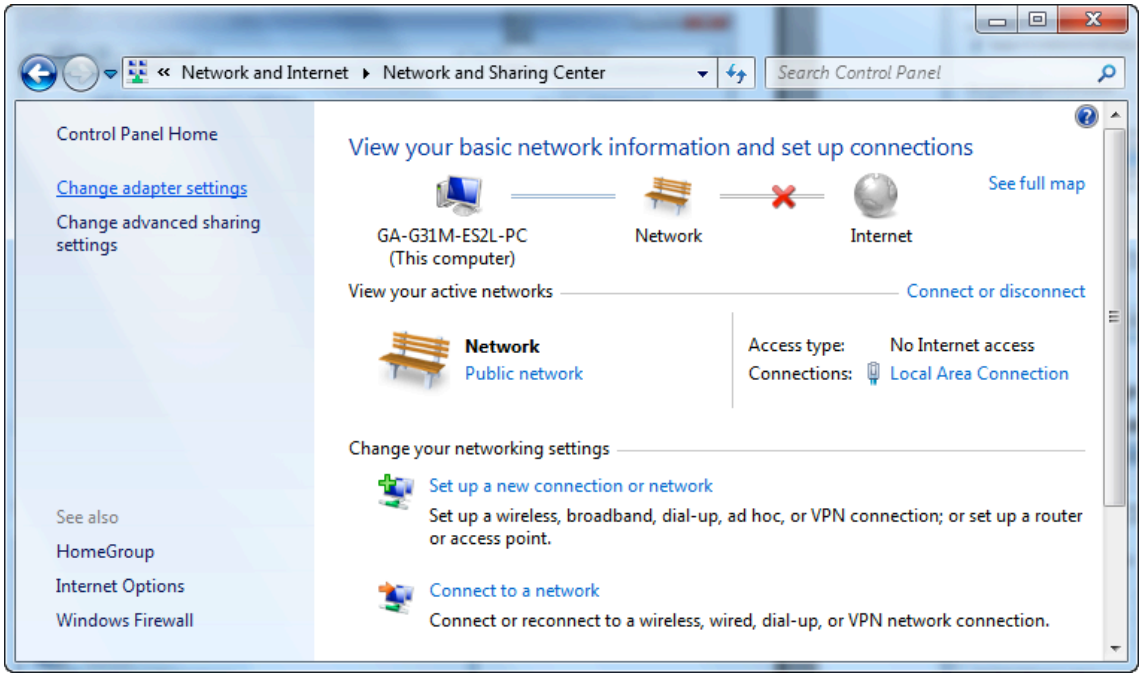
6. Selezionare "**Obtain an IP address automatically**" e "**Obtain DNS server address automatically**" e quindi premere "**OK**" per proseguire.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

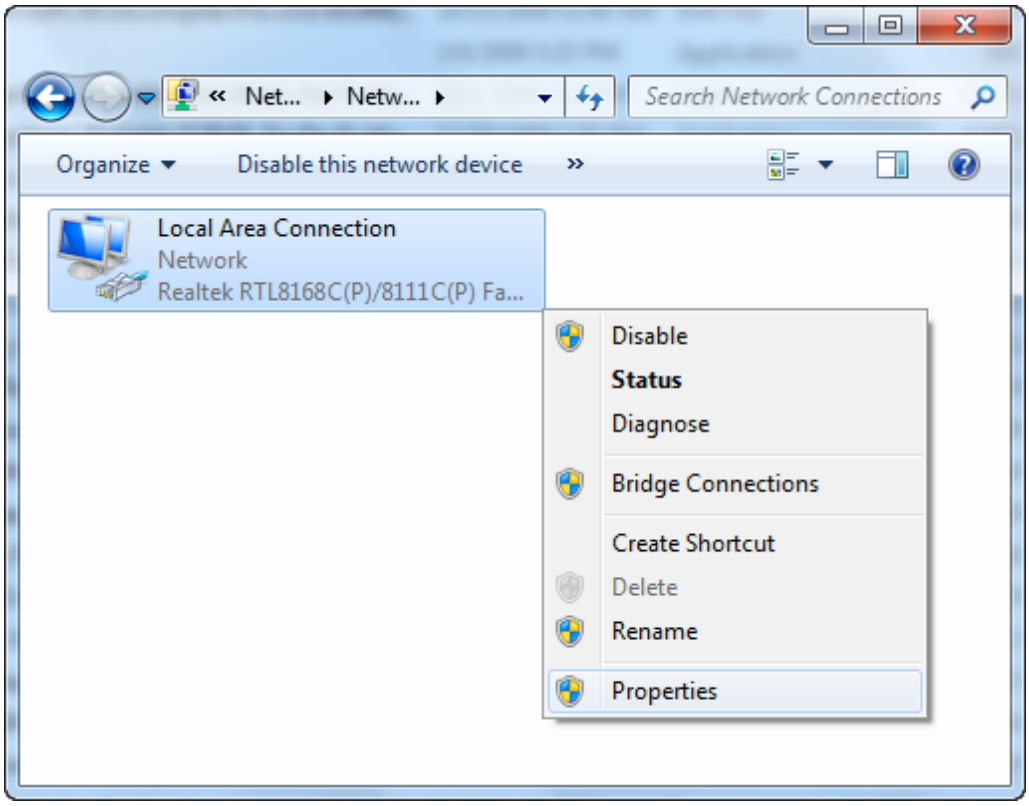
Windows 7-32/64

1. Fare click su “**Start**” -> “**Control Panel**” (in visualizzazione Categorie) -> “**View network status and tasks**”.

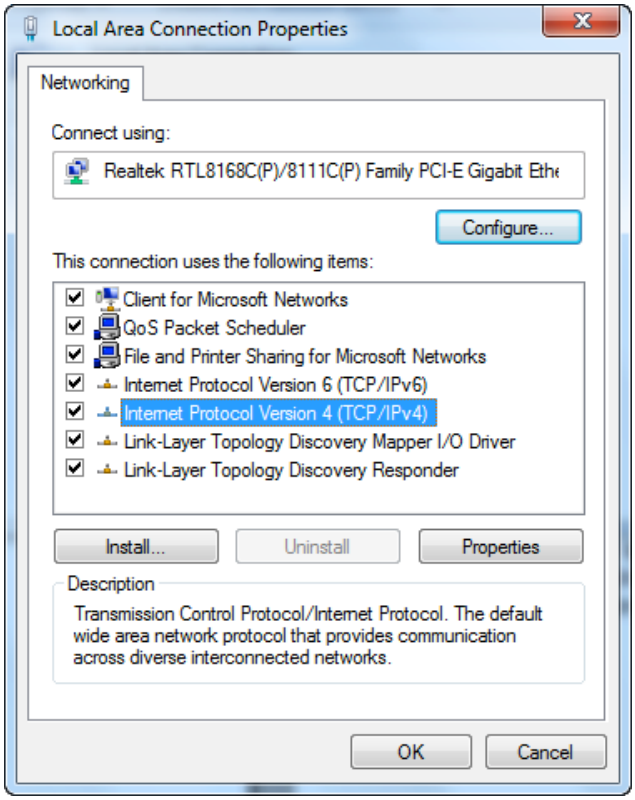
2. Nella sezione **Control Panel Home**, fare click su “**Change adapter settings**” per proseguire.


« Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
GA-G31M-ES2L-PC (This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Public network
Access type: No Internet access
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
See also
HomeGroup
Internet Options
Windows Firewall

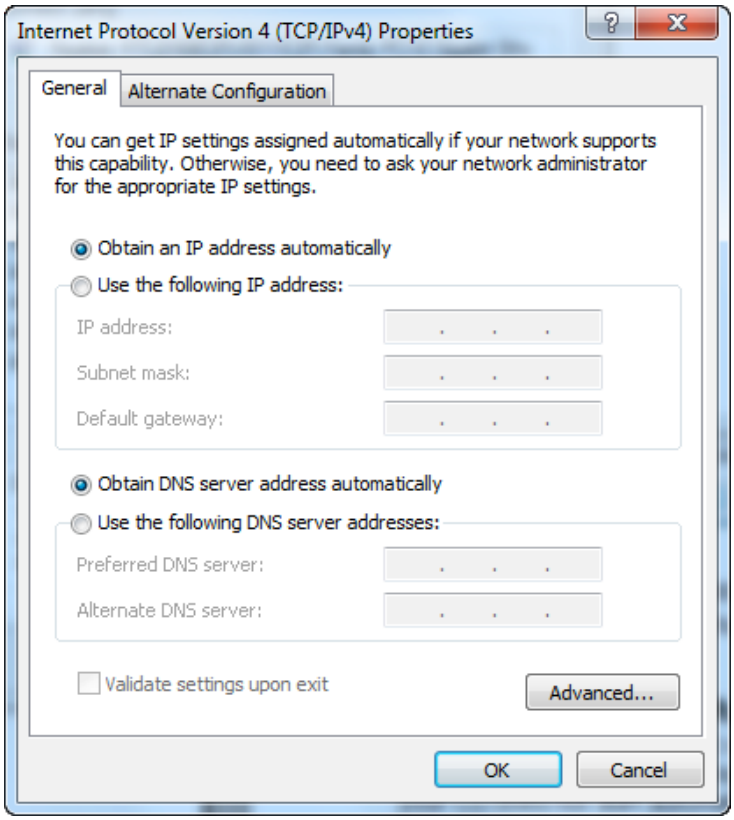
3. Selezionare con il tasto destro del mouse la voce "**Local Area connection**" e quindi selezionare "**Properties**" dal menù.



4. Fare doppio click su "**Internet Protocol Version 4 (TCP/IPv4)**".



5. Selezionare "**Obtain an IP address automatically**" e "**Obtain DNS server address automatically**" e quindi premere "**OK**" per proseguire.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

4 Collegamenti dell'apparato

Questo capitolo descrive le istruzioni necessarie per collegare il Router AP ad un computer o ad una rete LAN ed alla connessione Internet.

Sono fornite inoltre le istruzioni per impostare le proprietà della connessione Internet dal computer, operazione necessaria per configurare il Router AP. Per maggiori dettagli far riferimento alle successive sezioni:

- *Configurazione della connessione Ethernet sui PC*

Quanto descritto di seguito presuppone che si sia già attivata una connessione DSL con il proprio provider (ISP). Le seguenti istruzioni sono necessarie per configurare una rete di tipo "home" o "small office". Far riferimento ai seguenti sottoparagrafi per ulteriori istruzioni.

Collegamento dell'apparato

In questa sezione viene descritto come realizzare i collegamenti alla linea telefonica, alla rete elettrica ed al (ai) computer o alla rete LAN.

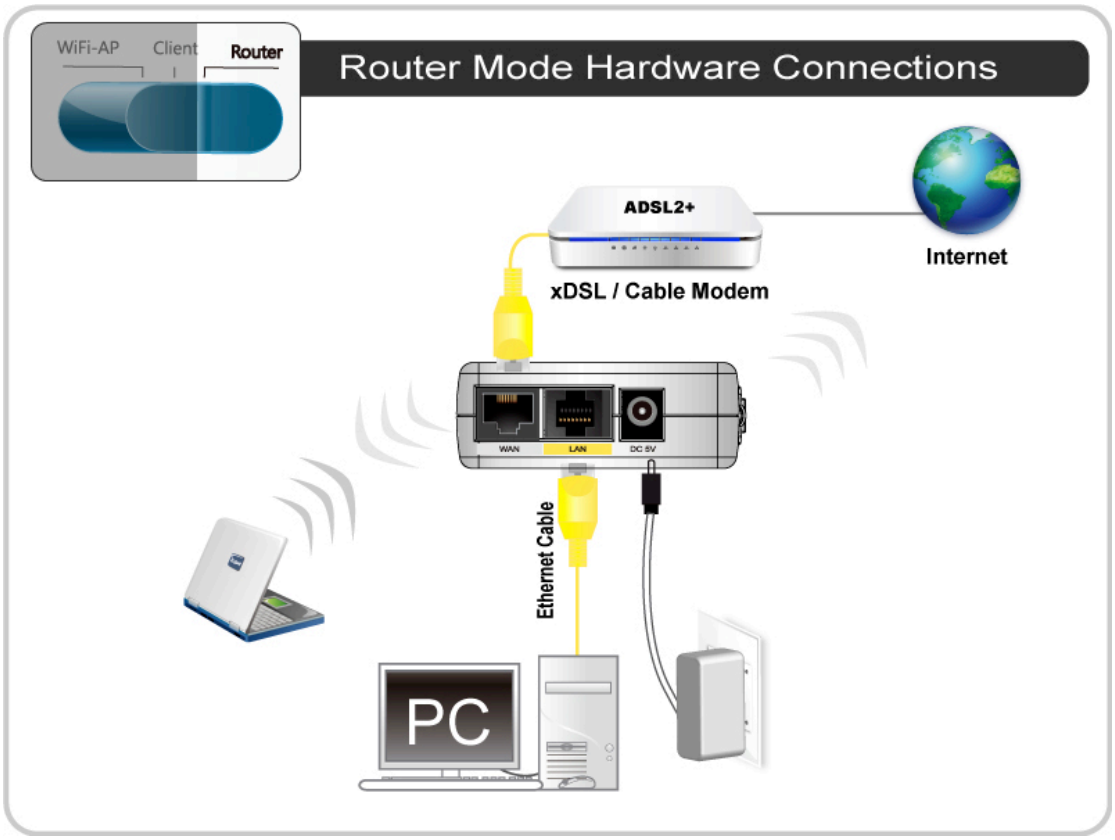
ATTENZIONE

***Prima di iniziare assicurarsi che tutti i dispositivi siano spenti**, incluso i computer, l' Hub/Switch della LAN (se presente) ed il Router.*

Il diagramma seguente illustra i collegamenti da realizzare. Si noti che la disposizione delle porte sul dispositivo potrebbe differire da quelle visualizzate, mantenendo comunque valida la descrizione. Far riferimento a quanto di seguito descritto.

Modalità Router (l'interfaccia WAN è connessa ad Internet mediante una connessione xDSL o un Modem di linea):

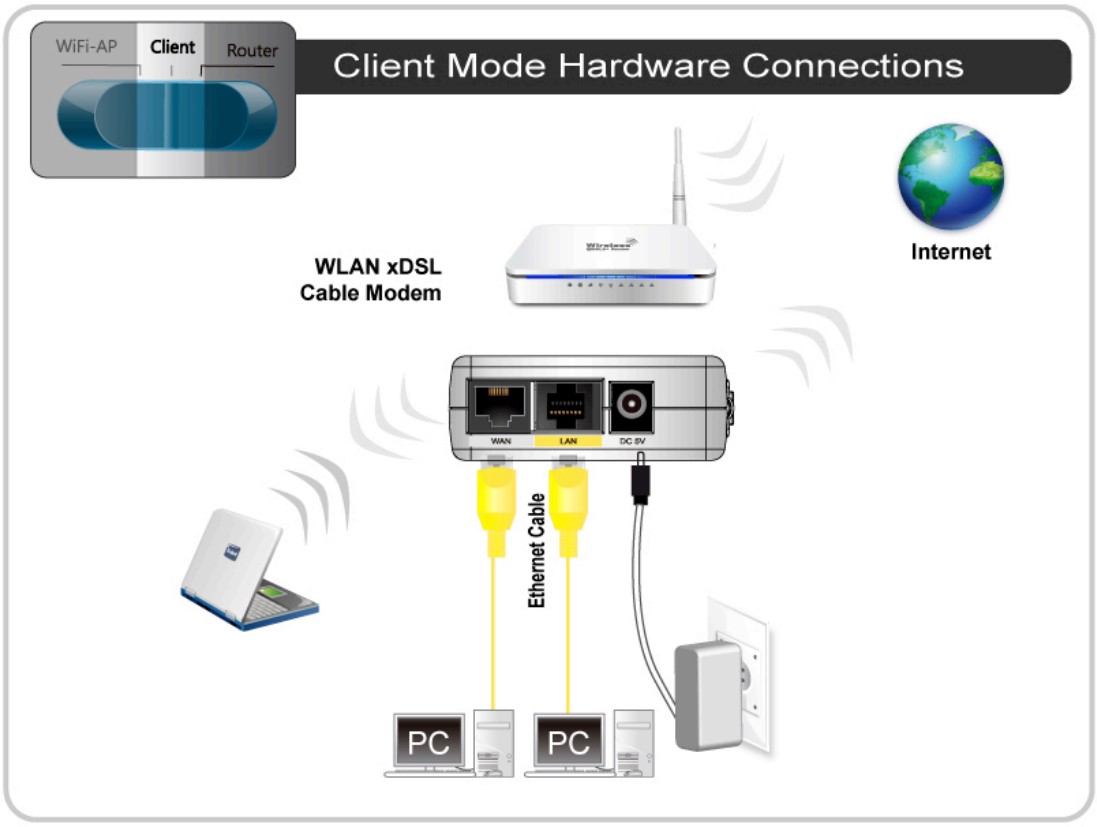
In questa modalità, il dispositivo si comporta come un router WLAN per connessioni xDSL o connessioni via Modem di linea.



1. Posizionare il commutatore delle modalità su **Router**
2. Collegare il cavo Ethernet alla porta WAN
   Collegare il cavo Ethernet RJ45 dalla porta Ethernet del modem xDSL o del Modem di Linea alla porta WAN del router 802.11n Pocket AP.
3. Collegare il cavo Ethernet alla porta LAN
   Collegare il cavo Ethernet RJ45 fornito in dotazione tra la porta Ethernet del PC e la porta LAN del Router 802.11n Pocket AP
4. Collegare l'adattatore di rete
   Collegare l'adattatore di rete al connettore POWER del modem 802.11n Pocket AP

Modalità Client (l'interfaccia WAN è connessa mediante un Router WLAN, xDSL o Modem di linea ad Internet):

In questa modalità il dispositivo si comporta come un router WLAN per connessioni xDSL o Modem di linea tramite l'interfaccia WLAN. (In tale modalità, la porta WAN funziona come una seconda porta LAN)



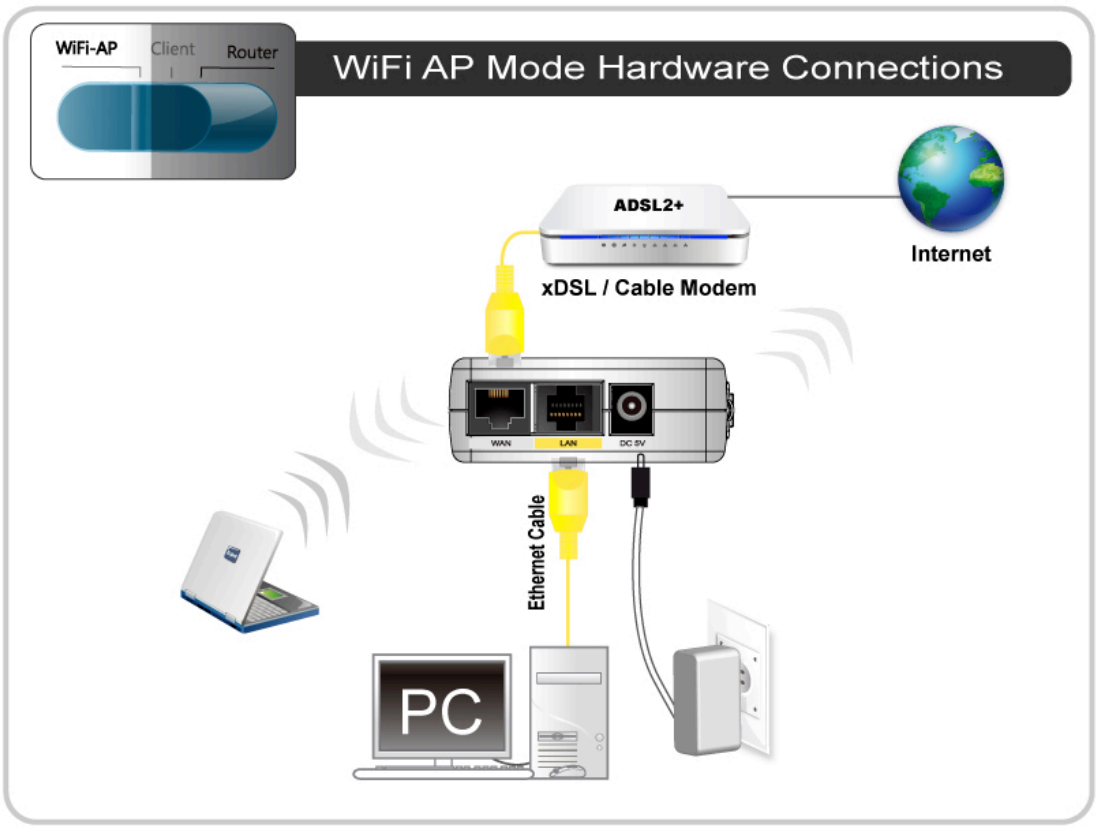
1. Posizionare il commutatore delle modalità su **Client**
2. Collegare il cavo Ethernet alla porta LAN e/o WAN

   Collegare il cavo Ethernet RJ45 fornito in dotazione tra la porta Ethernet del PC e la porta LAN o la porta WAN del Router 802.11n Pocket AP
3. Collegare l'adattatore di rete

   Collegare l'adattatore di rete al connettore POWER del modem 802.11n Pocket AP.

Modalità WiFi-AP (l'interfaccia WAN è connessa alla WAN, la porta LAN o l'interfaccia WLAN è connessa mediante Router WLAN, xDSL o Modem di Linea ad Internet):

In questa modalità, il dispositivo si comporta come un AP (Access Point) per connessioni xDSL o Modem di linea. (In tale modalità, la porta WAN funziona come una seconda porta LAN)



1. Posizionare il commutatore delle modalità su **WiFi-AP**
2. Collegare il cavo Ethernet alla porta WAN o LAN

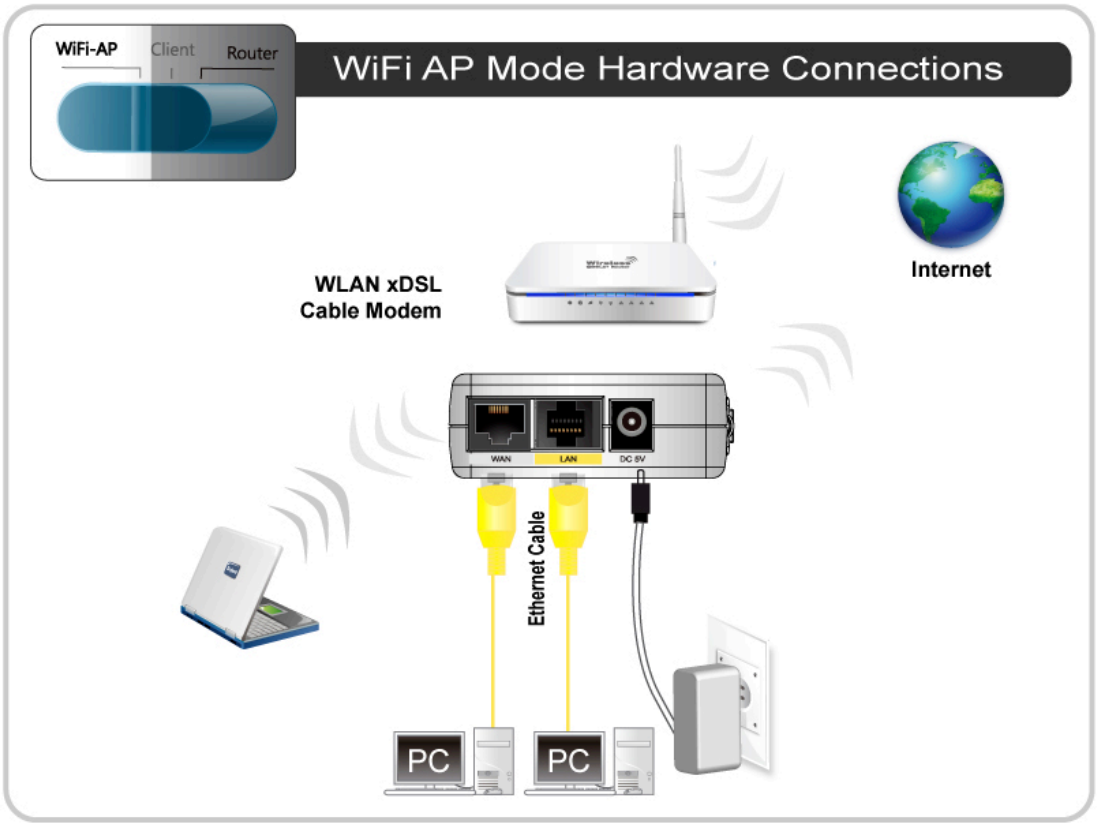
   Collegare il cavo Ethernet RJ45 dalla porta Ethernet del modem xDSL o del Modem di Linea alla porta WAN o alla porta LAN del router 802.11n Pocket AP.
3. Collegare il cavo Ethernet alla porta LAN o WAN

   Collegare il cavo Ethernet RJ45 fornito in dotazione tra la porta Ethernet del PC e la porta LAN o la porta WAN del Router 802.11n Pocket AP
4. Collegare l'adattatore di rete

   Collegare l'adattatore di rete al connettore POWER del modem 802.11n Pocket AP.

Modalità WiFi-AP (l'interfaccia WAN è connessa alla WAN, la porta LAN o l'interfaccia WLAN è connessa mediante Router WLAN, xDSL o Modem di linea ad Internet):

In questa modalità, il dispositivo si comporta come un AP (Access Point) per connessioni xDSL o Modem di linea. (In tale modalità, la porta WAN funziona come una seconda porta LAN)



1. Posizionare il commutatore delle modalità su **WiFi-AP**
2. Collegare il cavo Ethernet alla porta LAN o WAN

   Collegare il cavo Ethernet RJ45 fornito in dotazione tra la porta Ethernet del PC e la porta LAN o la porta WAN del Router 802.11n Pocket AP
3. Collegare l'adattatore di rete

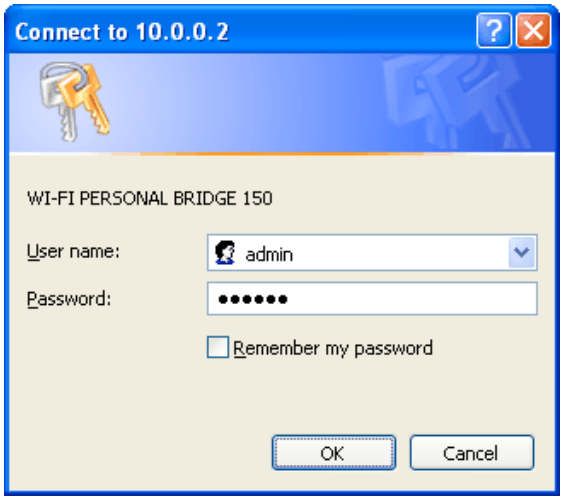
   Collegare l'adattatore di rete al connettore POWER del modem 802.11n Pocket AP.
4. Configurare il Router AP come Universal Repeater o come dispositivo WDS.

5 CD Utility

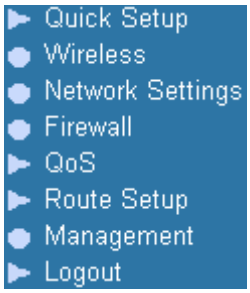
Configurazione avanzata per la modalità Router

1. Inserire il CD fornito nel lettore del PC.
2. Il CD si dovrebbe avviare automaticamente (modalità Auto-Start), visualizzando la schermata sottostante. Se il CD non si avvia automaticamente, aprire Risorse del Computer, selezionare il Driver del CD e quindi fare doppio click su "**autorun.exe**".
3. Per configurare il dispositivo, selezionare "**Advanced Configuration**".

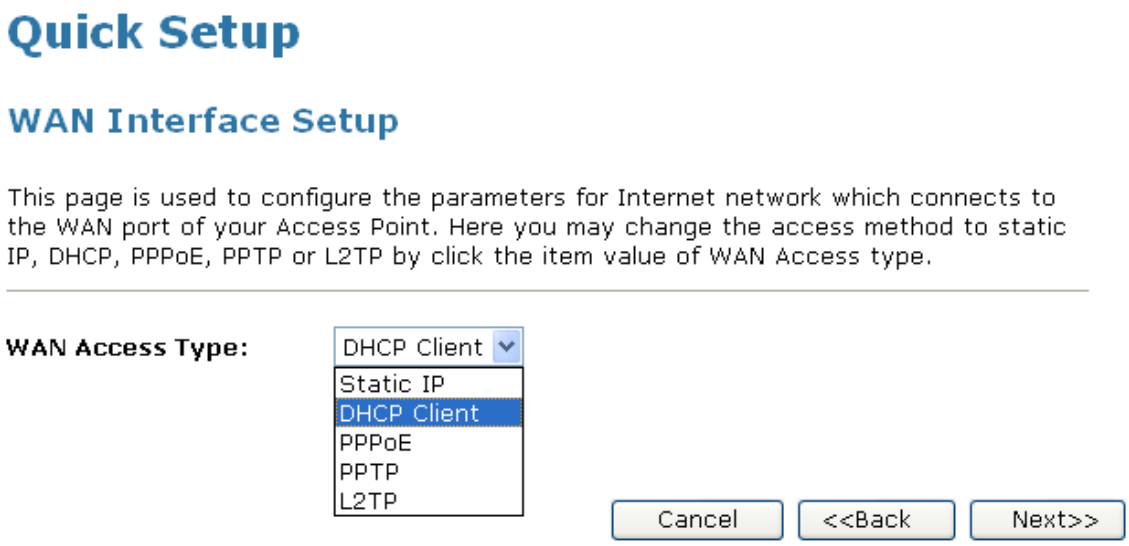
4. Nella finestra di Login digitare: User Name: **admin**, Password: **hamlet** e quindi confermare con il tasto **OK**.



5. Selezionare il menù **Quick Setup**.



6. Impostare il campo *WAN Access Type* come **DHCP Client**, **Static IP**, **PPPoE**, **PPTP** o **L2TP** ed inserire i relativi parametri forniti dal vostro ISP (Internet Services Provider) o dall'Amministratore di Rete e quindi premere il pulsante **Next>>**.

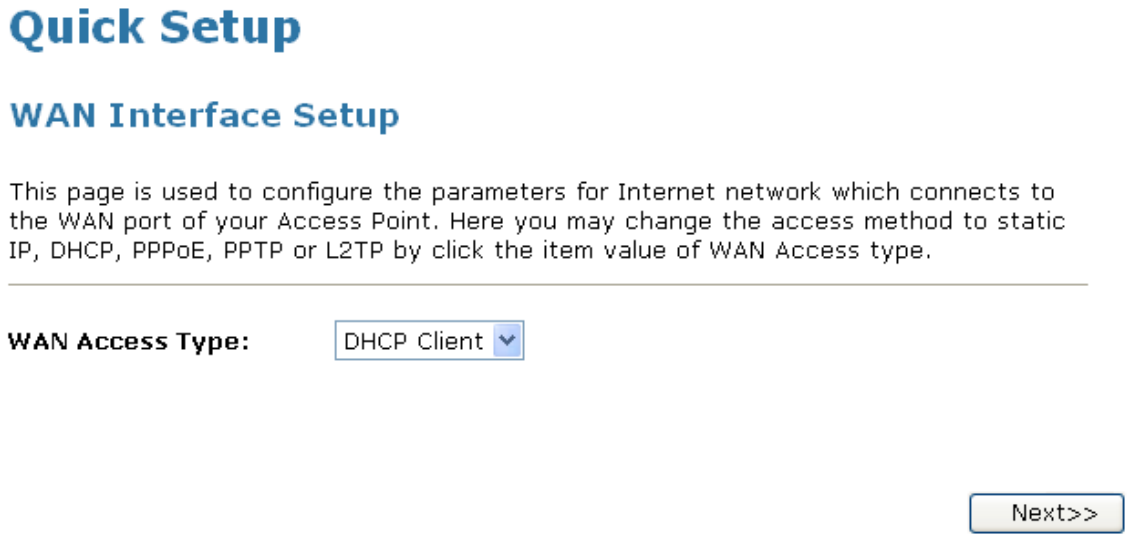

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Static IP
DHCP Client
PPPoE
PPTP
L2TP
Cancel
<<Back
Next>>

Esempi

6-1. DHCP Client

*Selezionare la modalità **DHCP Client** nel campo WAN Access Type.*

*Premere il pulsante **Next>>***

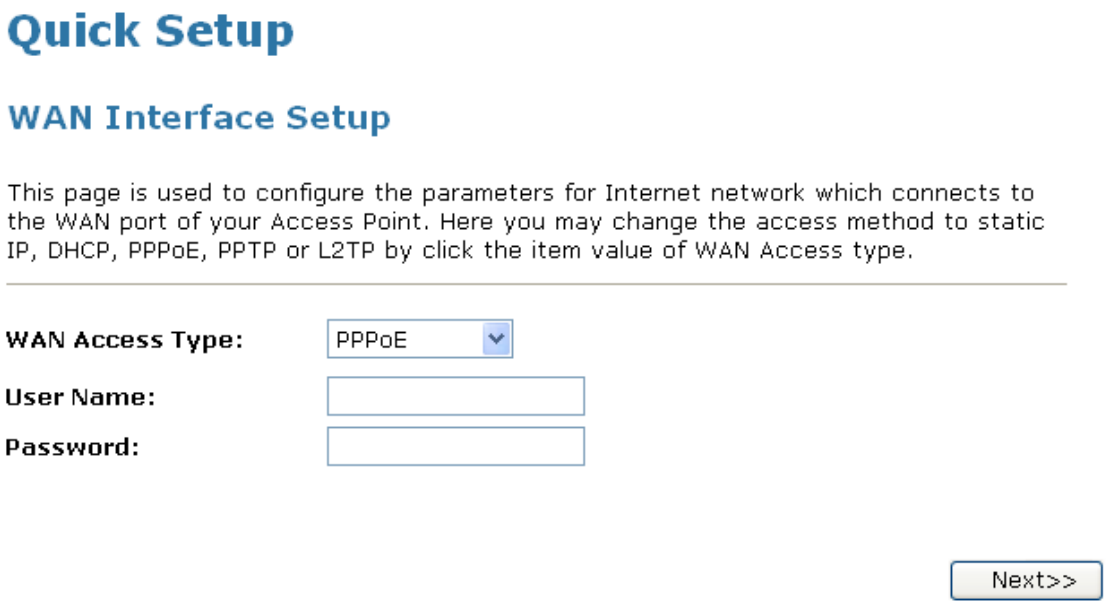

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Next>>

6-2. PPPoE

*Selezionare la modalità **PPPoE** nel campo WAN Access Type*

*Digitare **Username** e **Password** forniti dall'ISP*

*Premere il pulsante **Next>>***

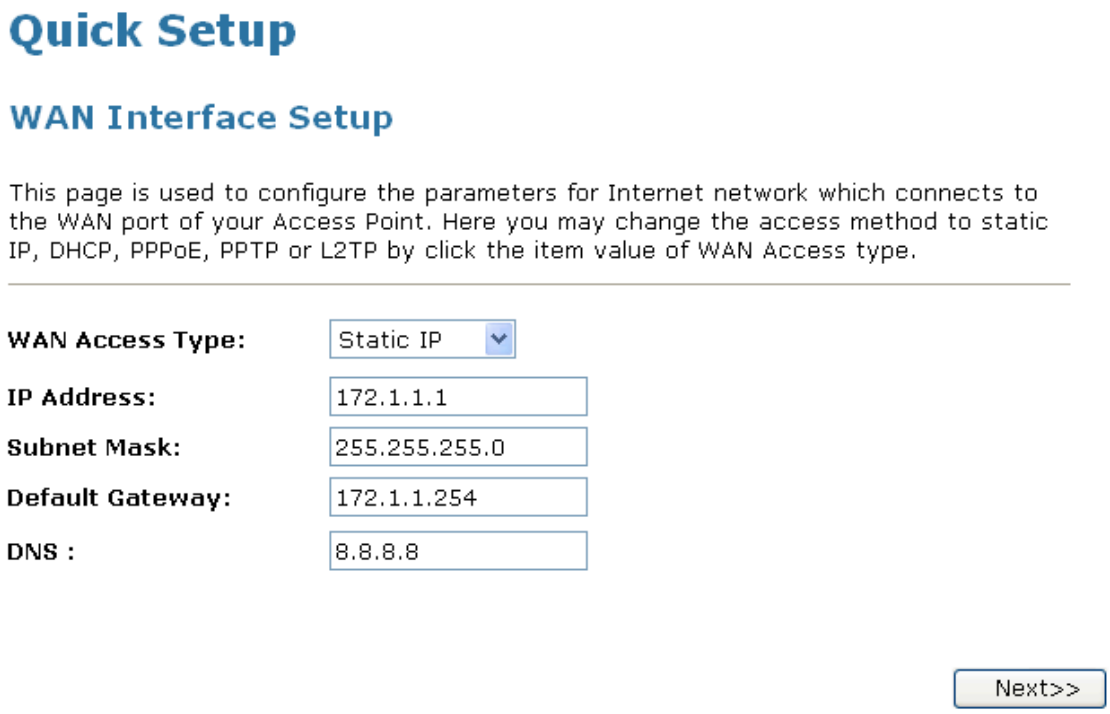

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
PPPoE
User Name:
Password:
Next>>

6-3. IP Statico

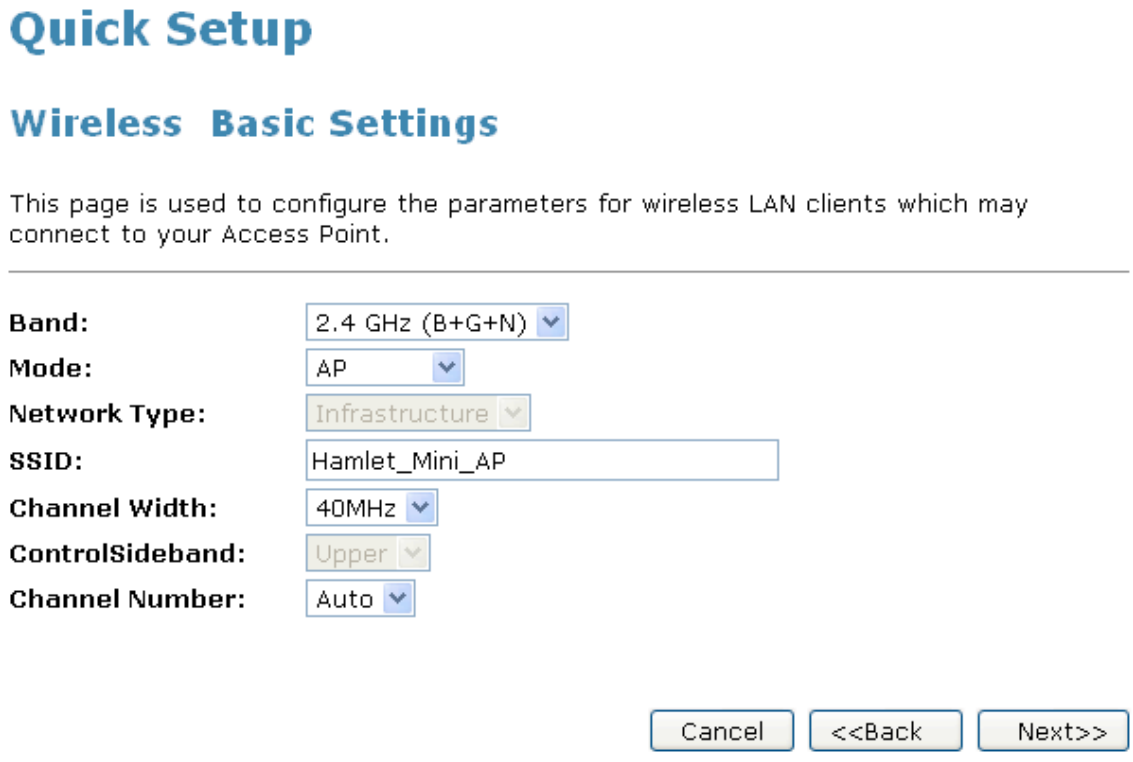
*Selezionare la modalità **Static IP** nel campo WAN Access Type*

*Configurare l'**indirizzo IP**, la **Subnet mask**, il **Default Gateway** ed il **DNS Server** secondo i dati forniti dall' ISP (Internet Services Provider) o dall'Amministratore di rete.*

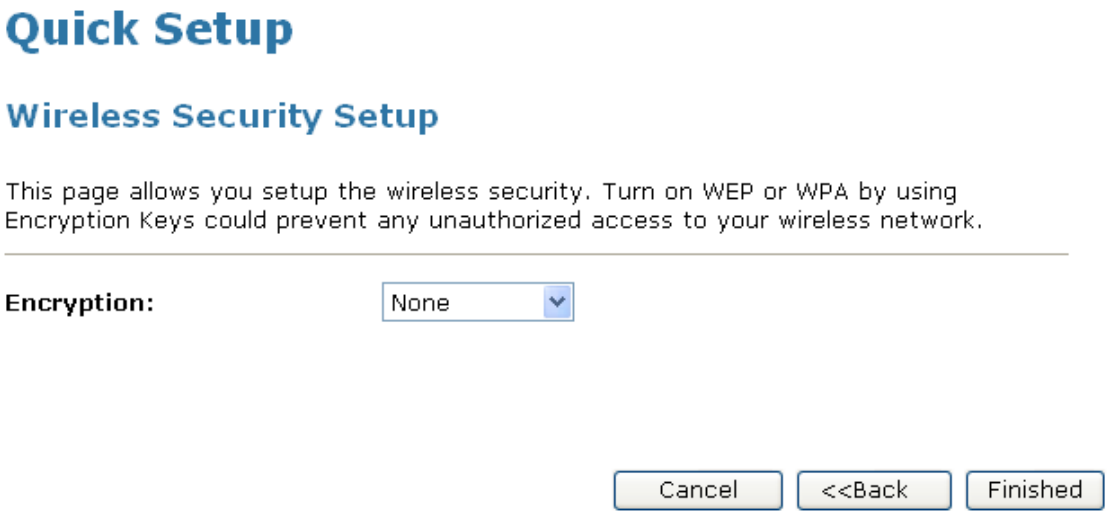
*Premere il pulsante **Next>>***


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
Static IP
IP Address:
172.1.1.1
Subnet Mask:
255.255.255.0
Default Gateway:
172.1.1.254
DNS :
8.8.8.8
Next>>

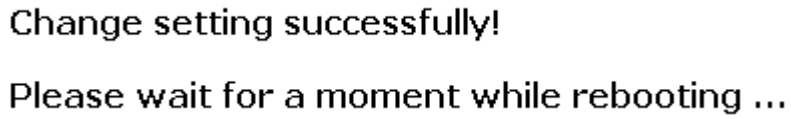
7. Digitare un nuovo valore nel campo "**SSID**",se si vuole cambiare quello di default (**SSID = Hamlet_Mini_AP**).
8. Premere il pulsante **Next>>**



9. Se necessario, modificare il campo *Encryption* selezionando uno dei seguenti valori: **None – No Encryption** / 64 Bit Encryption / 128 Bit Encryption / Wi-Fi Protected Access (AES-CCMP) / Wi-Fi Protected Access2 (AES-CCMP) e WPA2 Mixed. Ad esempio si può selezionare **None**.
10. Premere il pulsante **Finished**


Quick Setup
Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using
Encryption Keys could prevent any unauthorized access to your wireless network.
Encryption:
None
Cancel
<<Back
Finished

11. Si visualizza il messaggio:
Le modifiche sono state correttamente effettuate!
Attendere che il dispositivo si riavvii ...



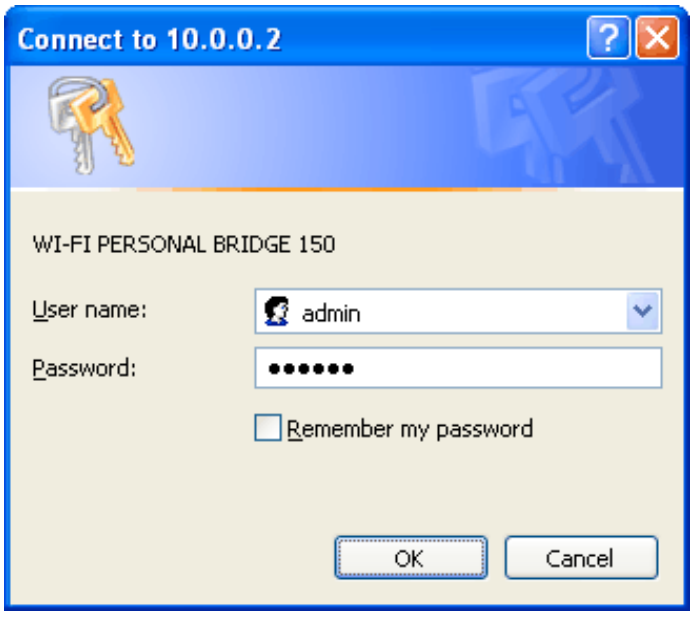
12. Premere " **Esci** " per terminare il programma.

13. In tal modo, il Router 802.11n Pocket AP è stato completamente configurato ed è pronto per effettuare connessioni Wireless e la connessione ad Internet.

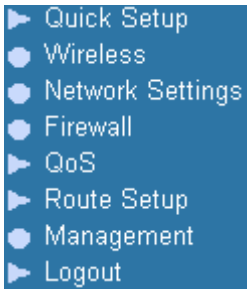
Configurazione avanzata in modalità Client

1. Inserire il CD fornito nel lettore del PC.
2. Il CD si dovrebbe avviare automaticamente (modalità Auto-Start), visualizzando la schermata sottostante. Se il CD non si avvia automaticamente, aprire Risorse del Computer, selezionare il Driver del CD e quindi fare doppio click su "**autorun.exe**".
3. Per configurare il dispositivo, selezionare "**Advanced Configuration**".

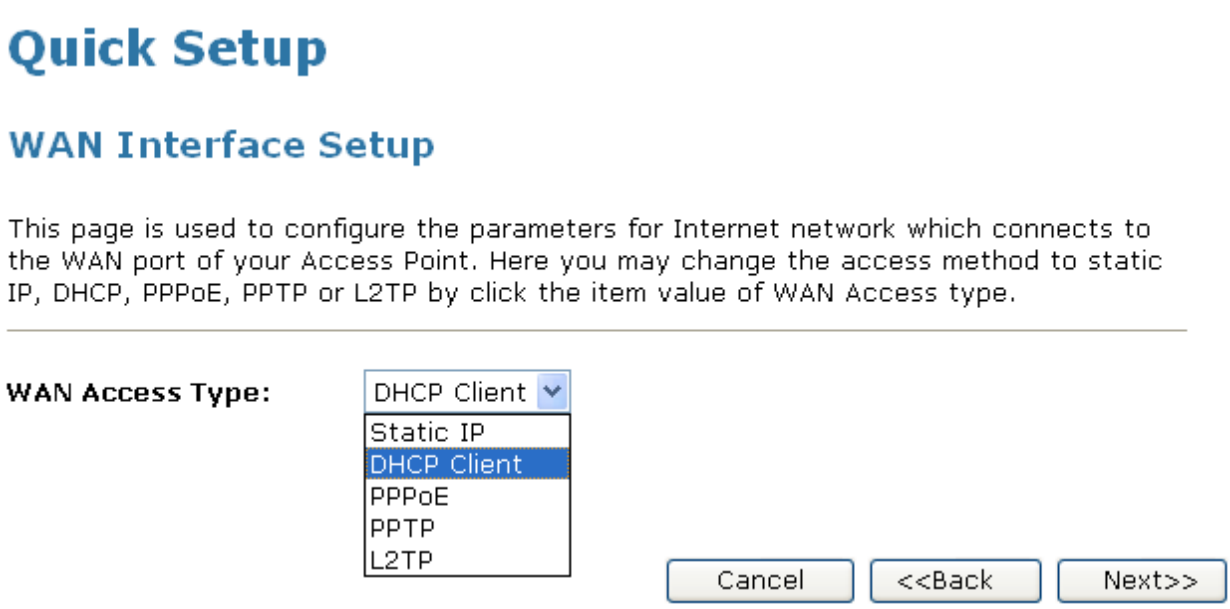
4. Nella finestra di Login digitare: User Name: **admin**, Password: **hamlet** e quindi confermare con il tasto **OK**.



5. Selezionare il menù **Quick Setup**.



6. Impostare il campo *WAN Access Type* come **DHCP Client**, **Static IP**, **PPPoE**, **PPTP** o **L2TP** ed inserire i relativi parametri forniti dal vostro ISP (Internet Services Provider) o dall'Amministratore di Rete e quindi premere il pulsante **Next>>**.

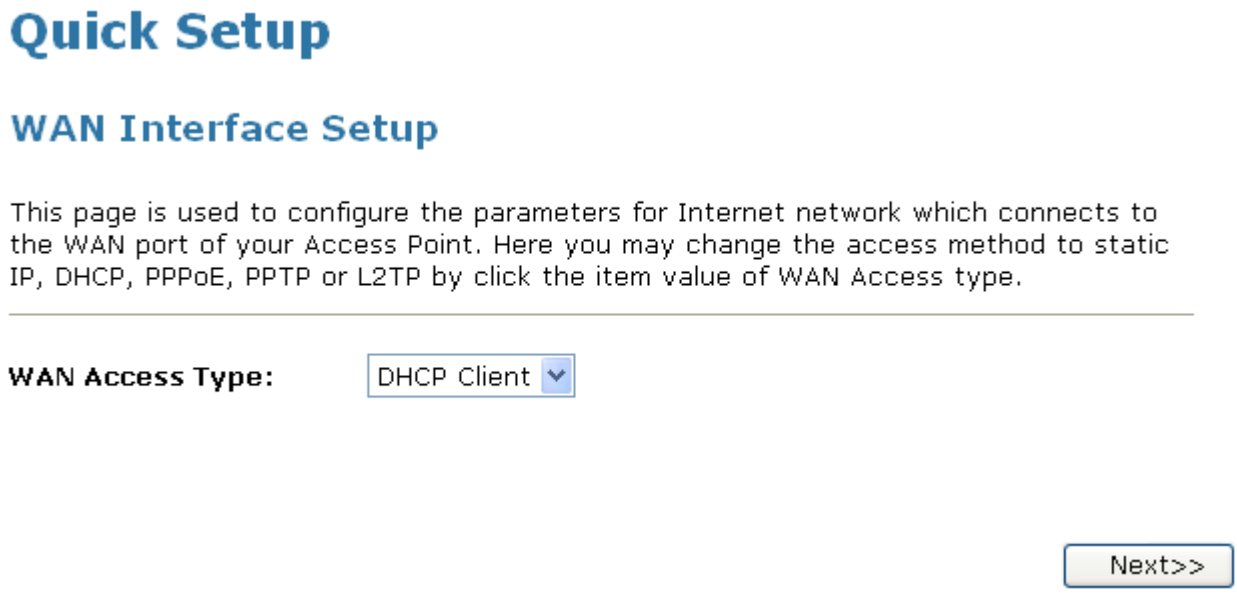

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Static IP
DHCP Client
PPPoE
PPTP
L2TP
Cancel
<<Back
Next>>

Esempi

6-1. DHCP Client

*Selezionare la modalità **DHCP Client** dall'elenco del campo WAN Access Type*

*Premere il pulsante **Next>>***

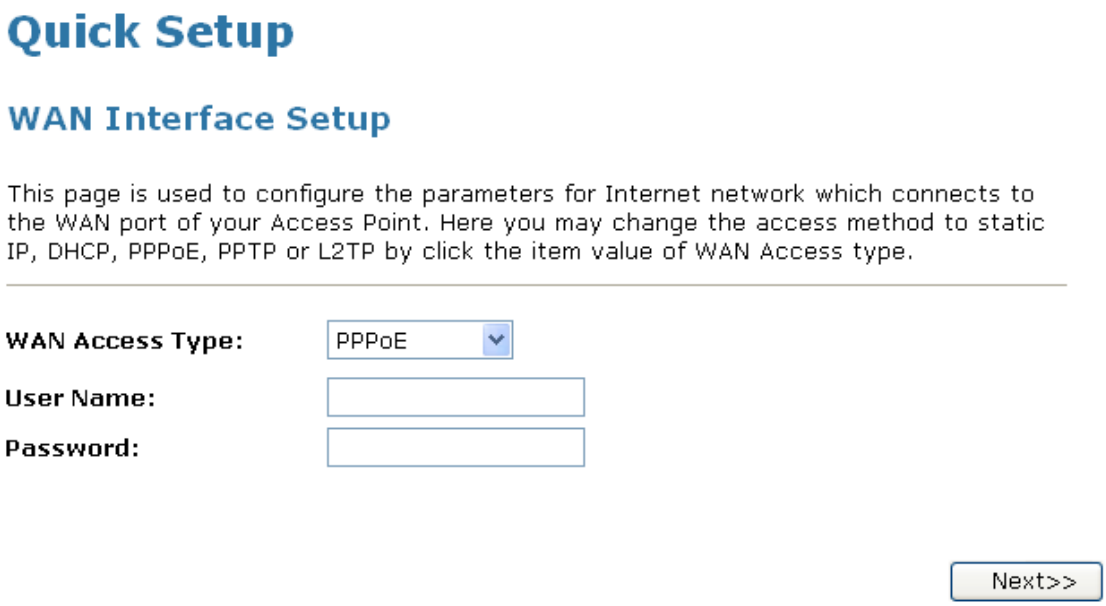

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Next>>

6-2. PPPoE

*Selezionare la modalità **PPPoE** dall'elenco del campo WAN Access Type*

*Digitare **Username** e **Password** forniti dall' ISP*

*Premere il pulsante **Next>>***

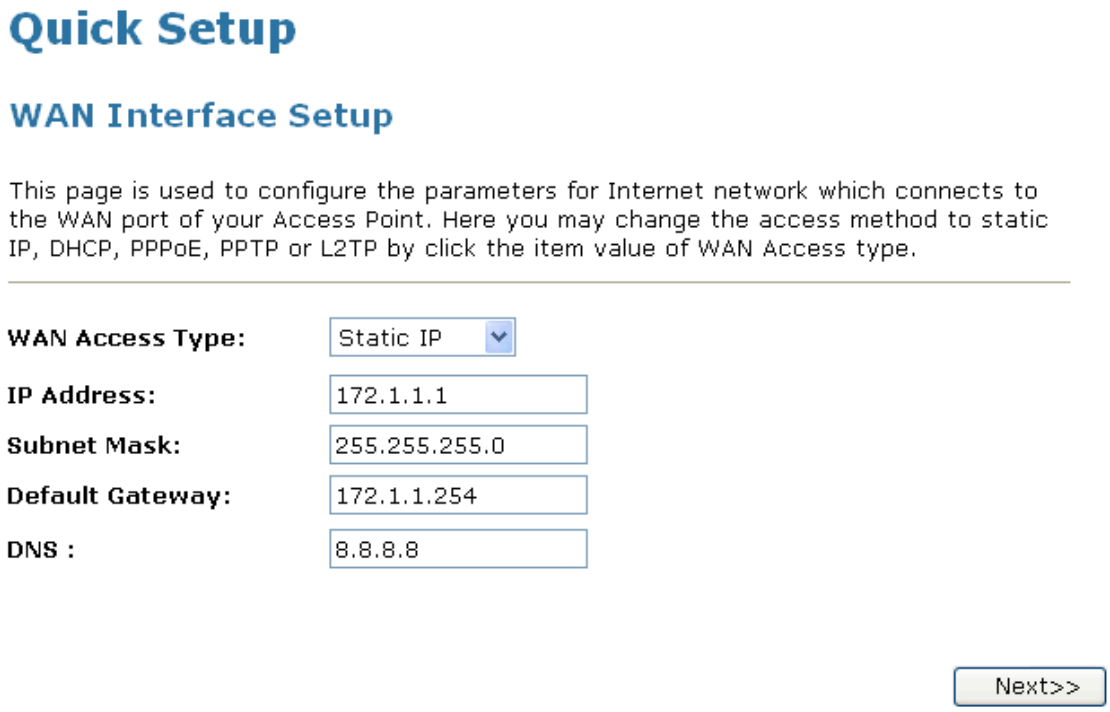

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
PPPoE
User Name:
Password:
Next>>

6-3. Static IP

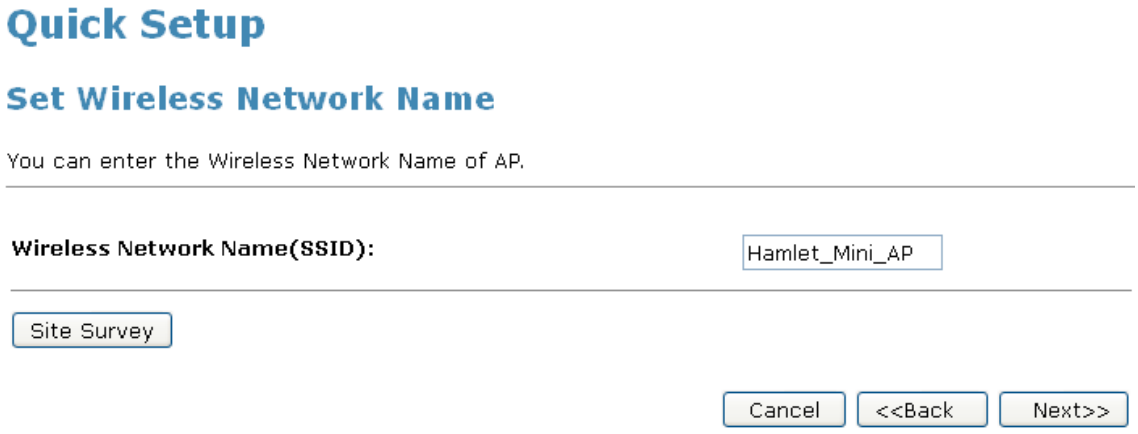
*Selezionare la modalità **Static IP** dall'elenco del campo WAN Access Type*

*Configurare l'**indirizzo IP**, la **Subnet mask**, il **Default Gateway** ed il **DNS Server** secondo i dati forniti dall' ISP (Internet Services Provider) o dall'Amministratore di rete*

*Premere il pulsante **Next>>***

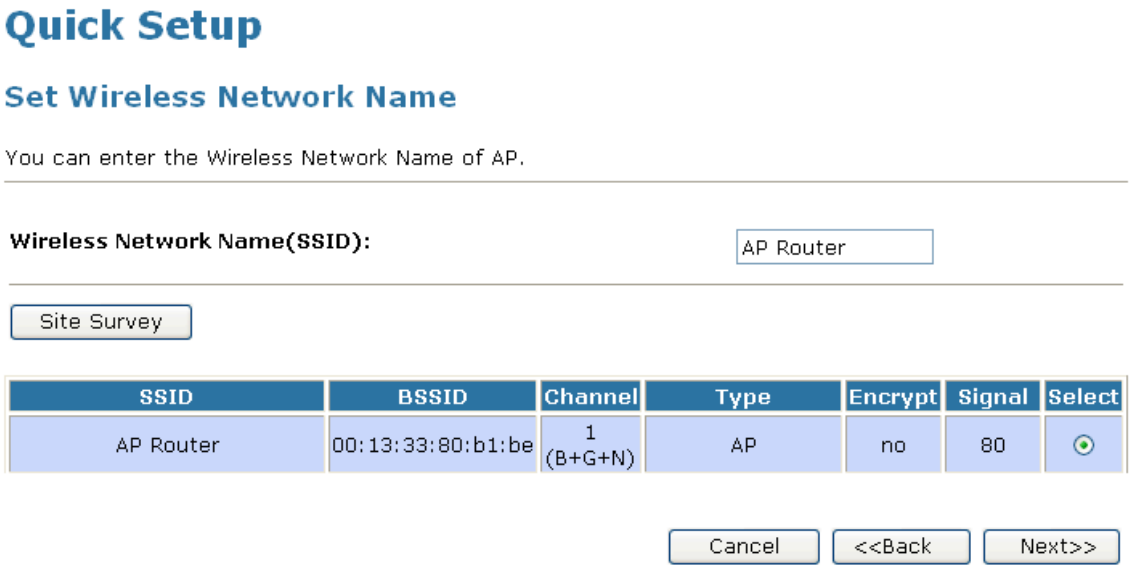

Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
Static IP
IP Address:
172.1.1.1
Subnet Mask:
255.255.255.0
Default Gateway:
172.1.1.254
DNS :
8.8.8.8
Next>>

7. Premere il pulsante **Site Survey**

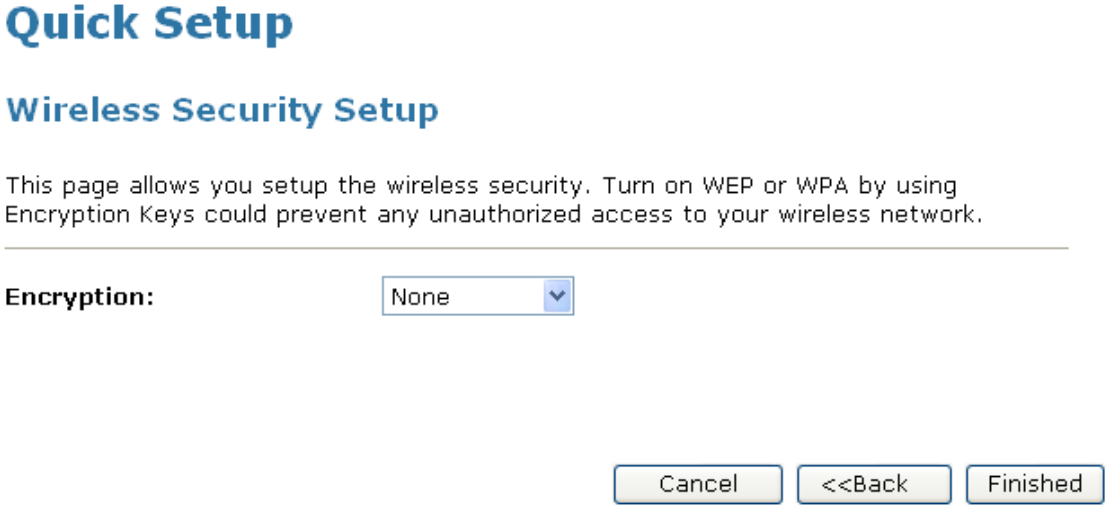


8. Selezionare l'identificativo SSID della rete Wireless del router.

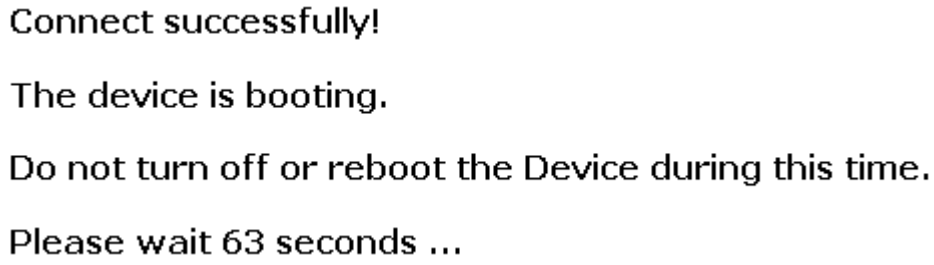
9. Premere il pulsante **Next>>**



10. Se necessario, modificare il campo *Encryption* selezionando uno dei seguenti valori: **None – No Encryption** / 64 Bit Encryption / 128 Bit Encryption / Wi-Fi Protected Access (AES-CCMP) / Wi-Fi Protected Access2 (AES-CCMP) e WPA2 Mixed. Ad esempio si può selezionare **None**.
11. Premere il pulsante **Finished**


Quick Setup
Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Encryption:
None
Cancel
<<Back
Finished

12. Si visualizza il messaggio: *Connessione effettuata correttamente! Il dispositivo si sta riavviando. Non spegnere o riavviare il dispositivo. Atendere 63 secondi ...*



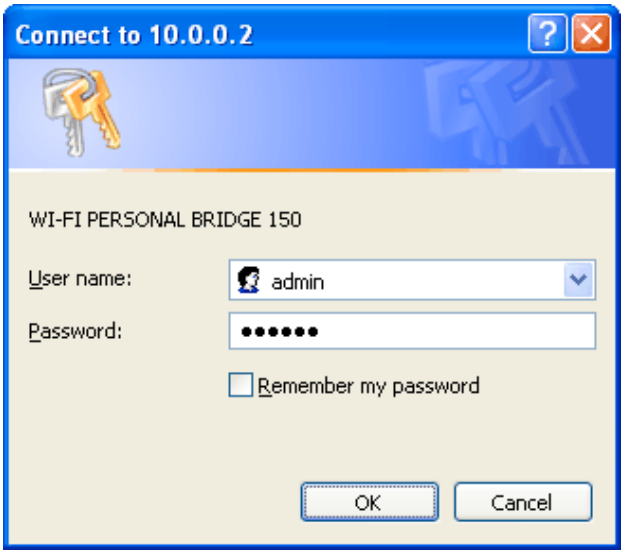
13. Premere " **Esci** " per terminare il programma.

14. In tal modo, il Router 802.11n Pocket AP e stato completamente configurato ed è pronto per permettere la connessione ad Internet.

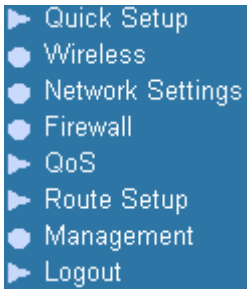
Configurazione avanzata per la modalità WiFi-AP Mode 1

1. Configurare sul PC un Adattatore Ethernet per avere un indirizzo IP fisso a 10.0.0.x (non utilizzare il valore 10.0.0.2).
2. Inserire il CD fornito nel lettore del PC.
3. Il CD si dovrebbe avviare automaticamente (modalità Auto-Start), visualizzando la schermata sottostante. Se il CD non si avvia automaticamente, aprire Risorse del Computer, selezionare il Driver del CD e quindi fare doppio click su "**autorun.exe**".
4. Per configurare il dispositivo, selezionare "**Advanced Configuration**".

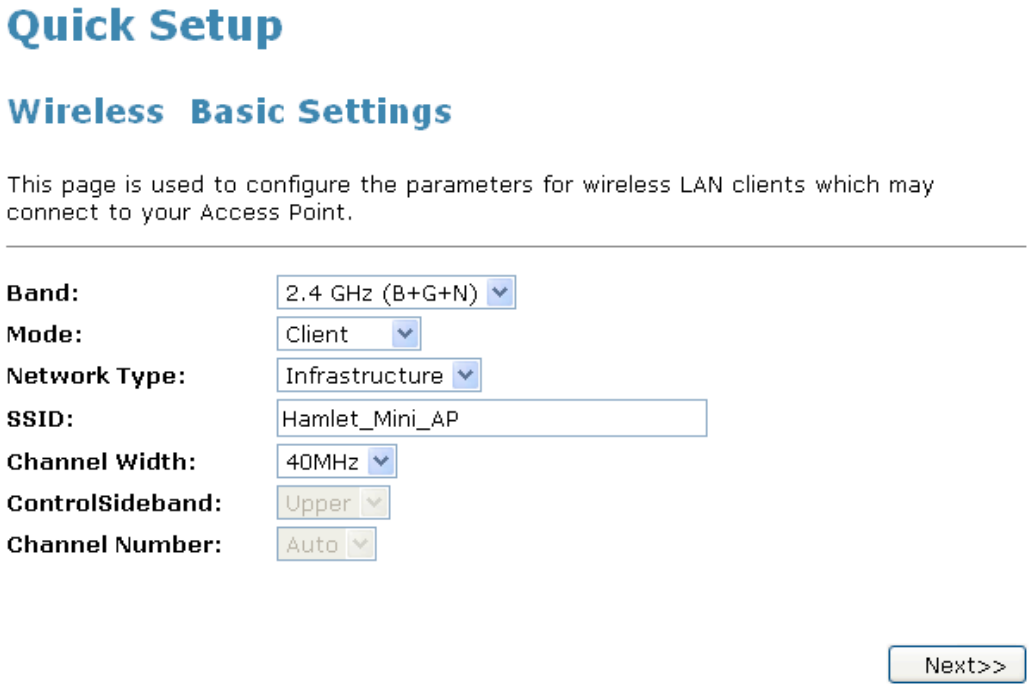
5. Nella finestra di Login digitare: User Name: **admin**, Password: **hamlet** e quindi confermare con il tasto **OK**.



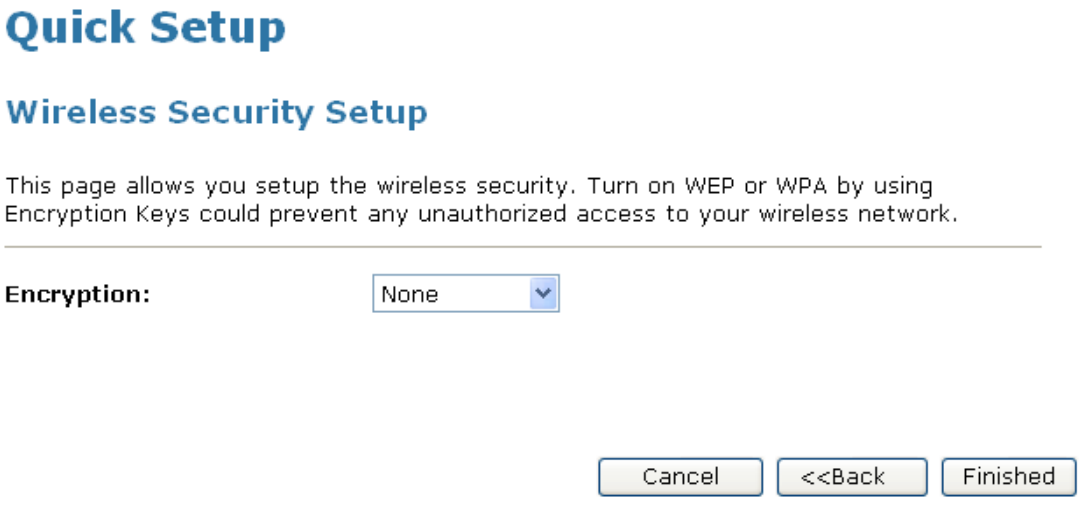
6. Selezionare il menù **Quick Setup**.



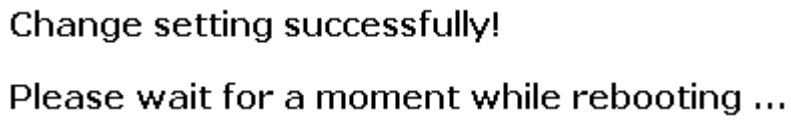
7. Selezionare **Client** dall'elenco delle modalità
8. Premere il pulsante **Next>>**



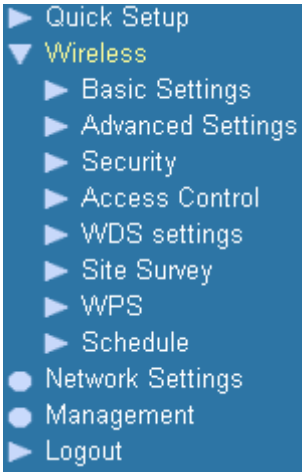
9. Se necessario, modificare il campo *Encryption* selezionando uno dei seguenti valori: **None – No Encryption** / 64 Bit Encryption / 128 Bit Encryption / Wi-Fi Protected Access (AES-CCMP) / Wi-Fi Protected Access2 (AES-CCMP) e WPA2 Mixed. Ad esempio si può selezionare **None**.
10. Premere il pulsante **Finished**


Quick Setup
Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Encryption:
None
Cancel
<<Back
Finished

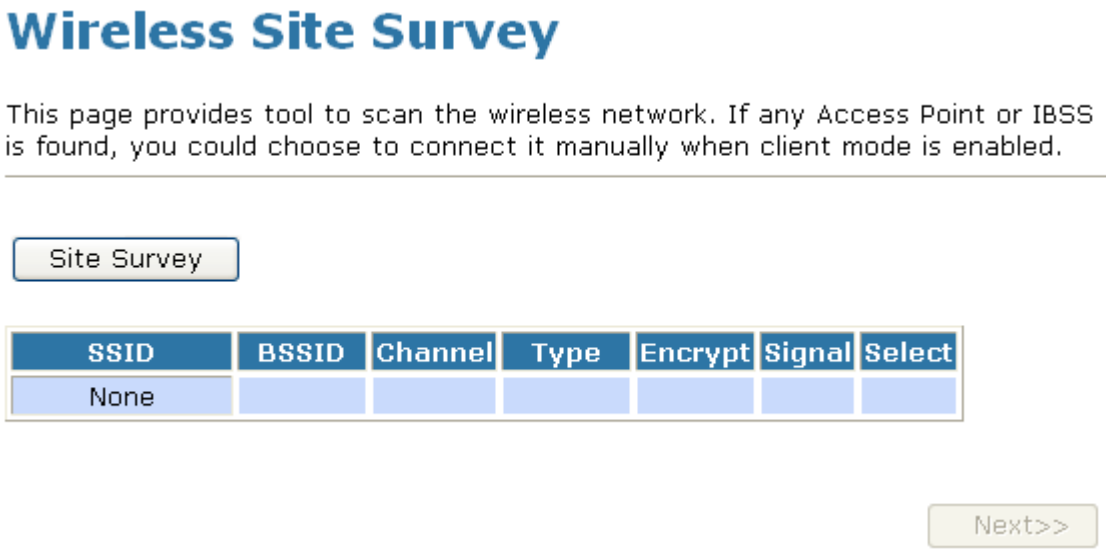
11. Si visualizza il messaggio: *Le modifiche sono state correttamente effettuate! Attendere che il dispositivo si riavvii ...*



12. Selezionare **Site Survey**

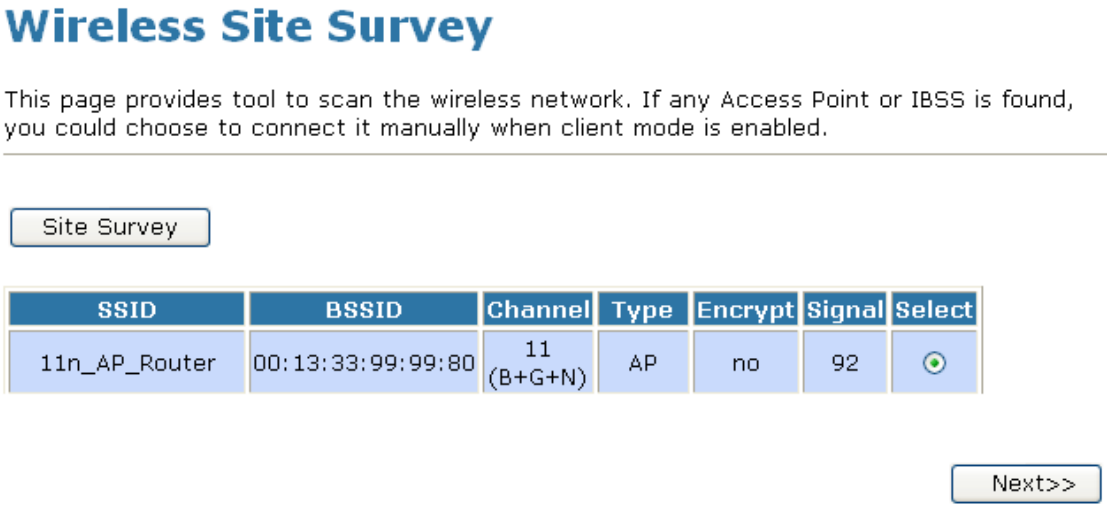


13. Premere il pulsante **Site Survey**

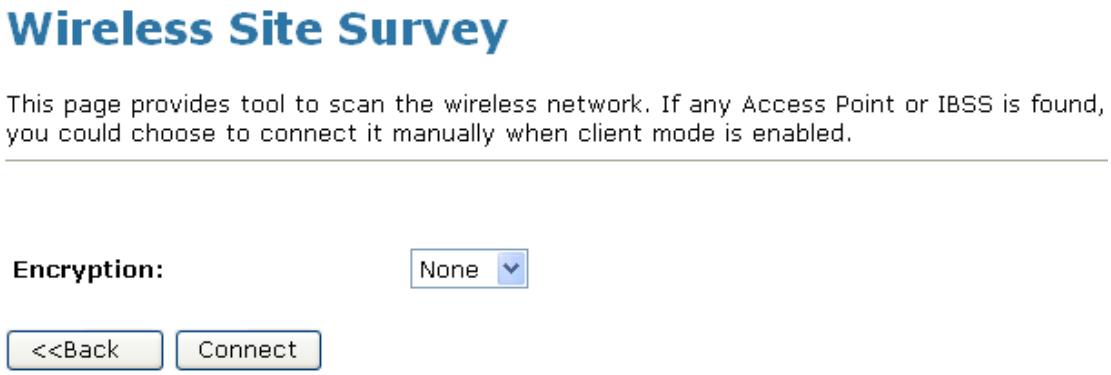


14. Selezionare l'identificativo SSID della rete Wireless del router.

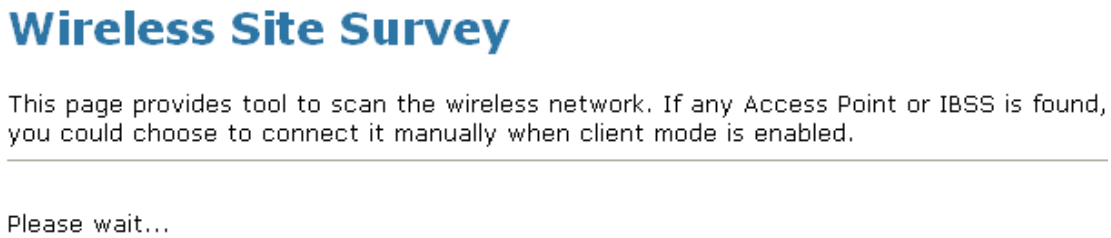
15. Premere il pulsante **Next>>**



16. Se necessario, modificare il campo *Encryption* selezionando uno dei seguenti valori: **None – No Encryption** / 64 Bit Encryption / 128 Bit Encryption / Wi-Fi Protected Access (AES-CCMP) / Wi-Fi Protected Access2 (AES-CCMP) e WPA2 Mixed. Ad esempio si può selezionare **None**.
17. Premere il pulsante **Connect**


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Encryption:
None
<<Back
Connect

18. Si visualizza il messaggio:
    Attendere…


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Please wait...

19. Si visualizza il messaggio: *Connessione effettuata correttamente! Il dispositivo si sta riavviando. Non spegnere o riavviare il dispositivo. Attendere 63 secondi ...*

Connect successfully!

The device is booting.

Do not turn off or reboot the Device during this time.

Please wait 63 seconds ...

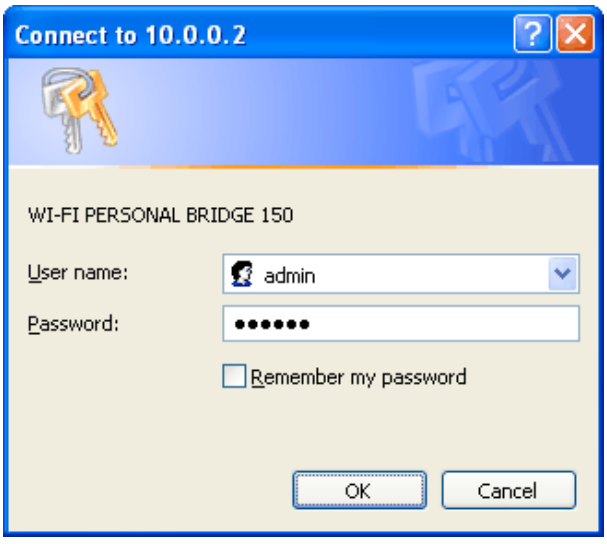
20. Premere " **Esci** " per terminare il programma.

21. In tal modo, il Router 802.11n Pocket AP e stato completamente configurato ed è pronto per permettere connessioni Wireless e connessioni ad Internet.

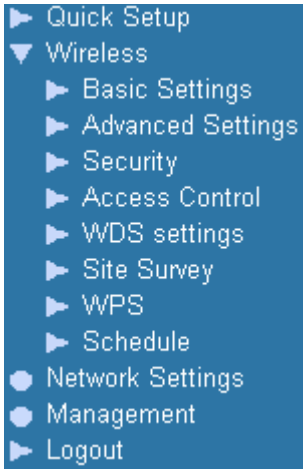
Configurazione avanzata per la modalità WiFi-AP Mode 2 - Universal Repeater (il Router opera come AP e Client contemporaneamente)

1. Configurare sul PC un Adattatore Ethernet per avere un indirizzo IP fisso a 10.0.0.x (non utilizzare il valore 10.0.0.2).
2. Inserire il CD fornito nel lettore del PC.
3. Il CD si dovrebbe avviare automaticamente (modalità Auto-Start), visualizzando la schermata sottostante. Se il CD non si avvia automaticamente, aprire Risorse del Computer, selezionare il Driver del CD e quindi fare doppio click su "**autorun.exe**".
4. Per configurare il dispositivo, selezionare "**Advanced Configuration**".

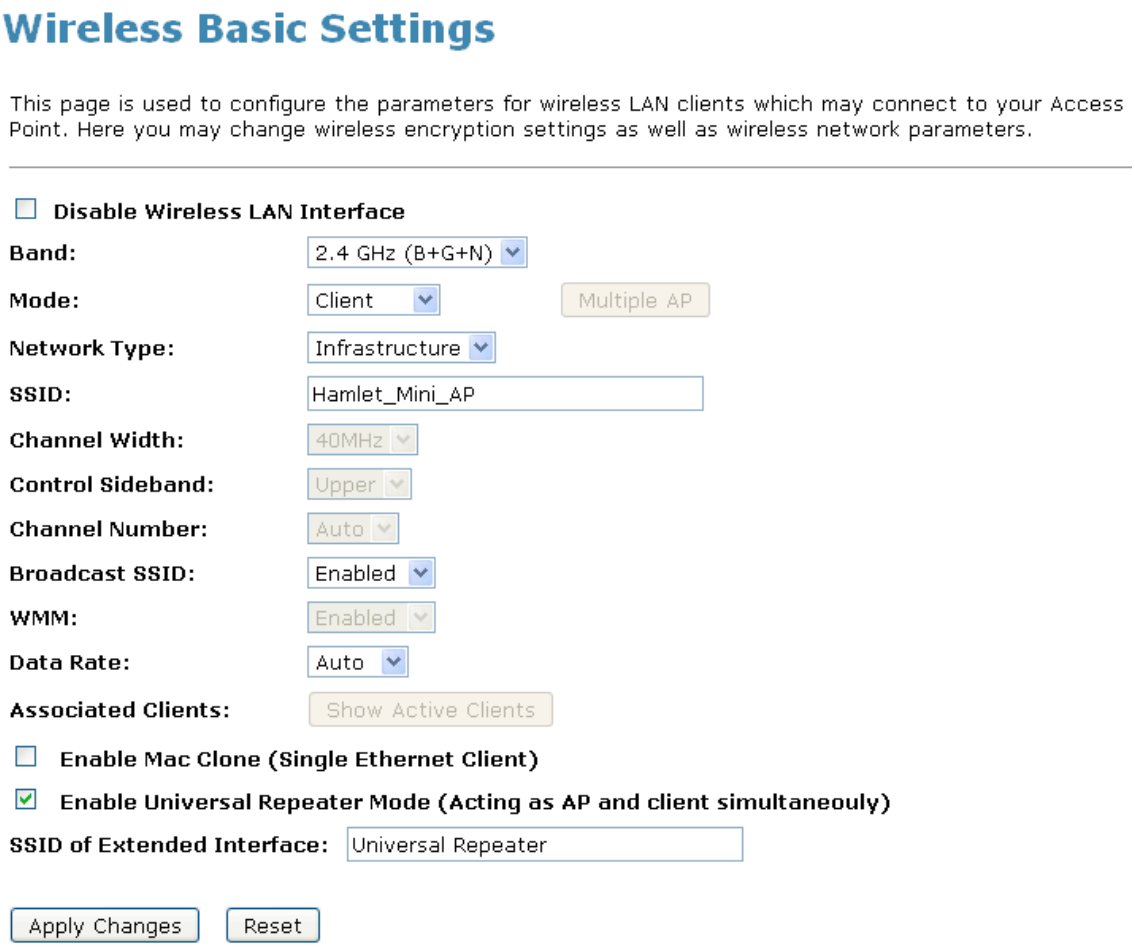
5. Nella finestra di Login digitare: User Name: **admin**, Password: **hamlet** e quindi confermare con il tasto **OK**.



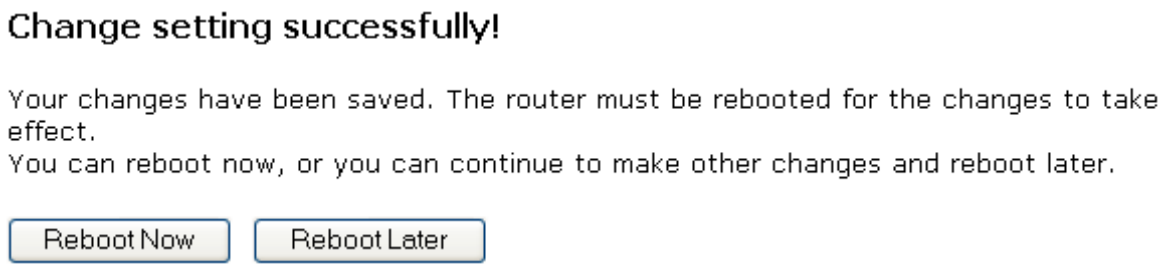
6. Selezionare il menù **Wireless -> Basic Settings**.



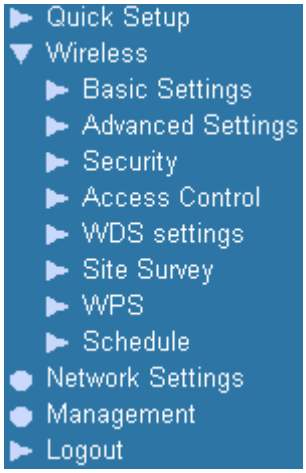
7. Selezionare **Client** dall'elenco delle modalità
8. Selezionare l'opzione **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**
9. Digitare il valore **SSID** nel campo **SSID of Extended Interface**
10. Premere il pulsante **Apply Changes**


Wireless Basic Settings
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.
Disable Wireless LAN Interface
Band: 2.4 GHz (B+G+N)
Mode: Client Multiple AP
Network Type: Infrastructure
SSID: Hamlet_Mini_AP
Channel Width: 40MHz
Control Sideband: Upper
Channel Number: Auto
Broadcast SSID: Enabled
WMM: Enabled
Data Rate: Auto
Associated Clients: Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface: Universal Repeater
Apply Changes
Reset

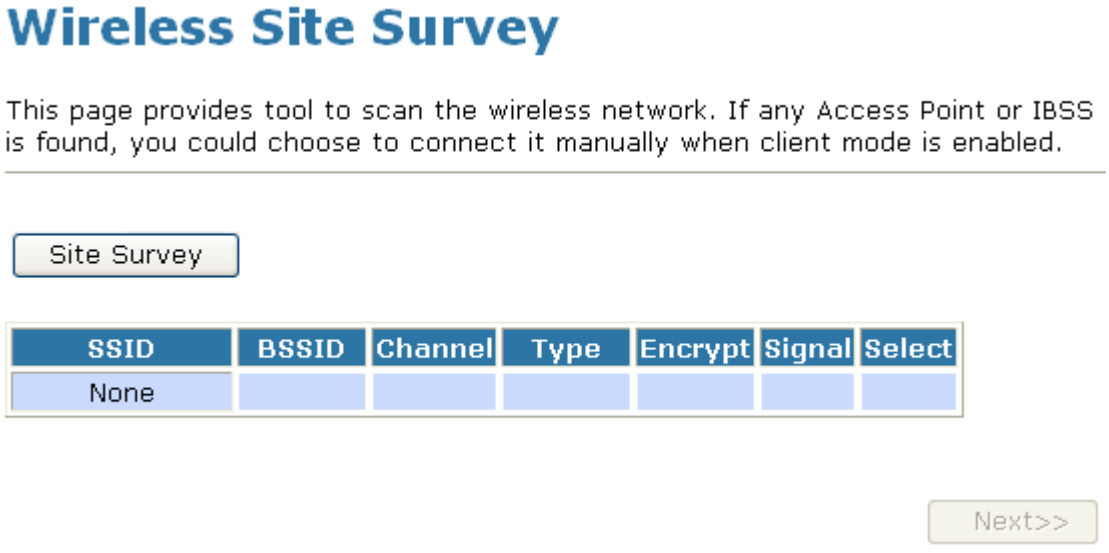
11. Premere il pulsante **Reboot Later**


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

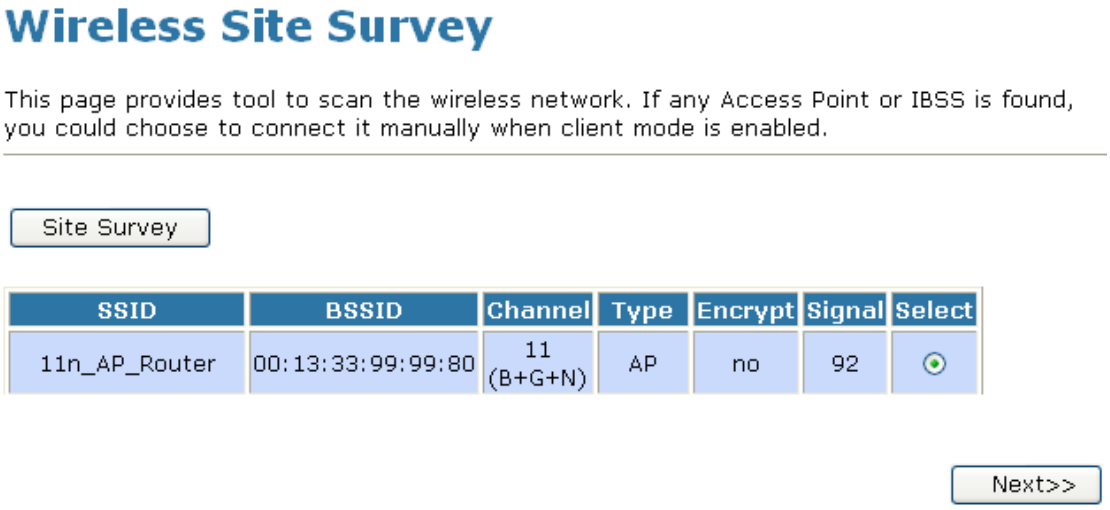
12. Selezionare il menù **Wireless -> Site Survey**.



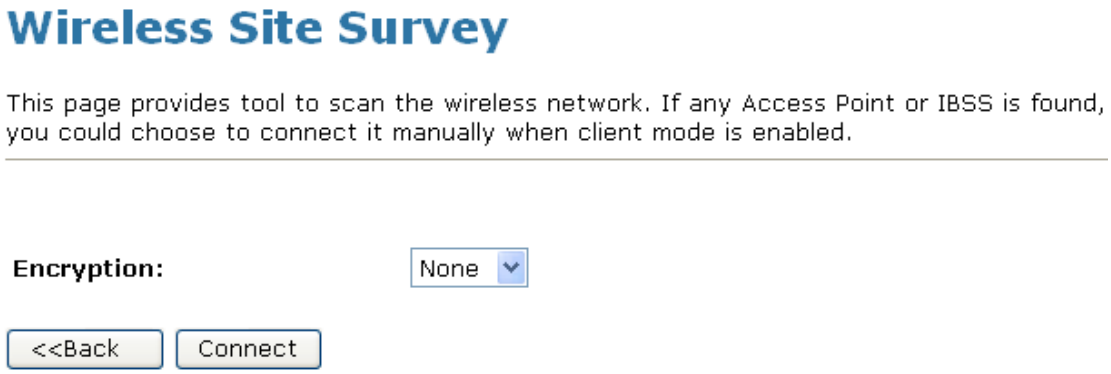
13. Premere il pulsante **Site Survey**



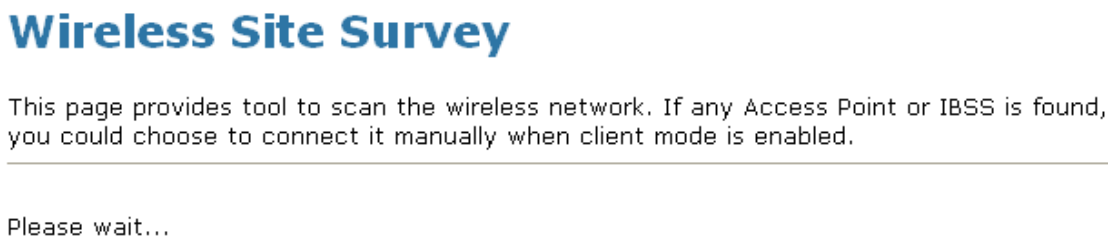
14. Selezionare l'identificativo **SSID** della rete Wireless del router.
15. Premere il pulsante **Next>>**



16. Se necessario, modificare il campo *Encryption* selezionando uno dei seguenti valori: **None – No Encryption** / 64 Bit Encryption / 128 Bit Encryption / Wi-Fi Protected Access (AES-CCMP) / Wi-Fi Protected Access2 (AES-CCMP) e WPA2 Mixed. Ad esempio si può selezionare **None**.
17. Premere il pulsante **Connect**


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Encryption:
None
<<Back
Connect

18. Si visualizza il messaggio:
    Attendere…


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Please wait...

19. Si visualizza il messaggio: *Connessione effettuata correttamente! Il dispositivo si sta riavviando. Non spegnere o riavviare il dispositivo. Attendere 63 secondi ...*

Connect successfully!

The device is booting.

Do not turn off or reboot the Device during this time.

Please wait 63 seconds ...

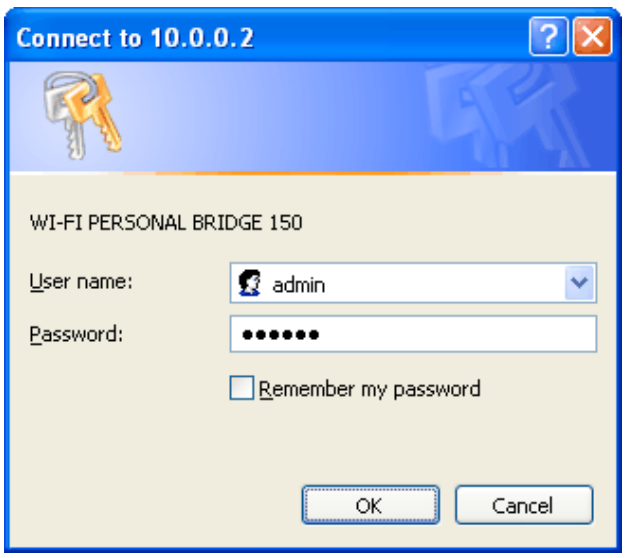
20. Premere " **Esci** " per terminare il programma.

21. In tal modo, il Router 802.11n Pocket AP e stato completamente configurato ed è pronto per permettere connessioni Wireless e connessioni ad Internet.

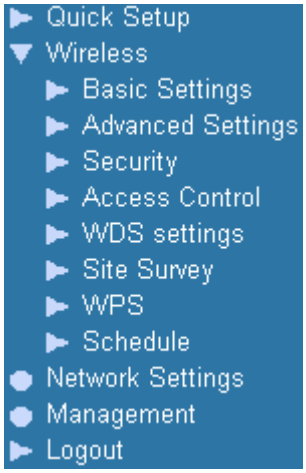
Configurazione avanzata per la modalità WiFi-AP Mode 3 - WDS

1. Configurare sul PC un Adattatore Ethernet per avere un indirizzo IP fisso a 10.0.0.x (non utilizzare il valore 10.0.0.2).
2. Inserire il CD fornito nel lettore del PC.
3. Il CD si dovrebbe avviare automaticamente (modalità Auto-Start), visualizzando la schermata sottostante. Se il CD non si avvia automaticamente, aprire Risorse del Computer, selezionare il Driver del CD e quindi fare doppio click su "**autorun.exe**".
4. Per configurare il dispositivo, selezionare "**Advanced Configuration**".

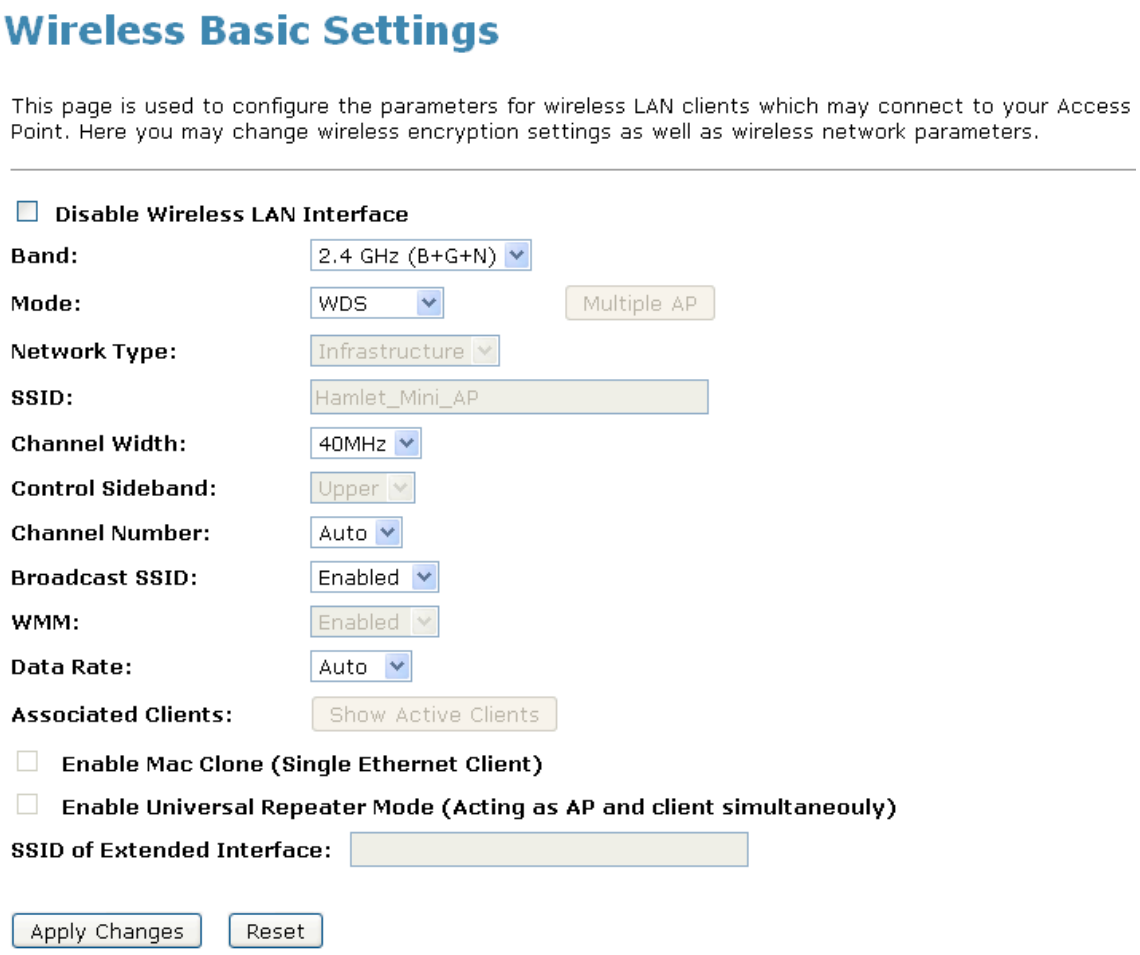
5. Nella finestra di Login digitare: User Name: **admin**, Password: **hamlet** e quindi confermare con il tasto **OK**.



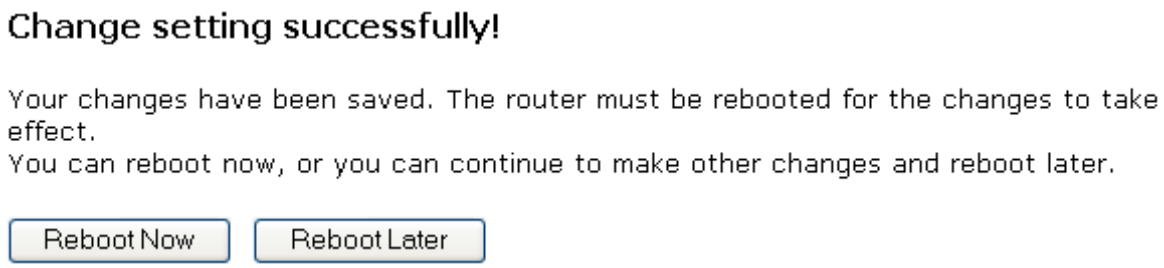
6. Selezionare il menù **Wireless -> Basic Settings**.



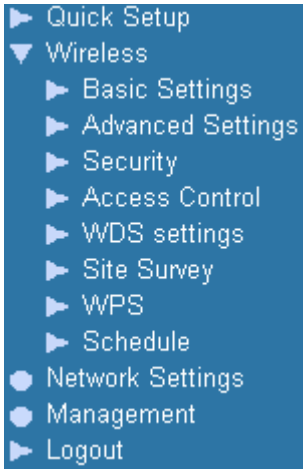
7. Selezionare **WDS** dall'elenco del campo **Mode**
8. Impostare il valore per **Channel Width**
9. Impostare il valore per **Control Sideband**
10. Impostare il valore per **Channel Number**
11. Premere il pulsante **Apply Changes**



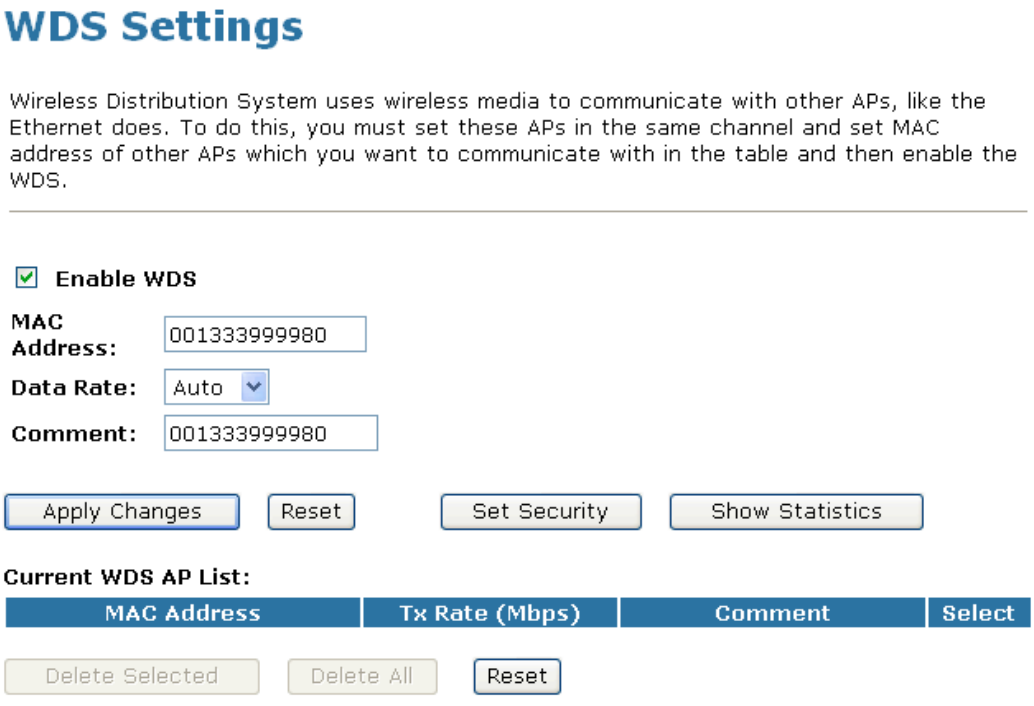
12. Premere il pulsante **Reboot Later**


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

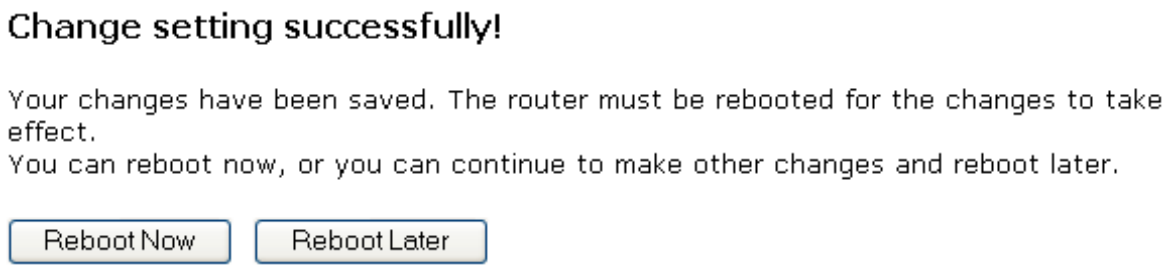
13. Selezionare il menù **Wireless -> WDS settings**.



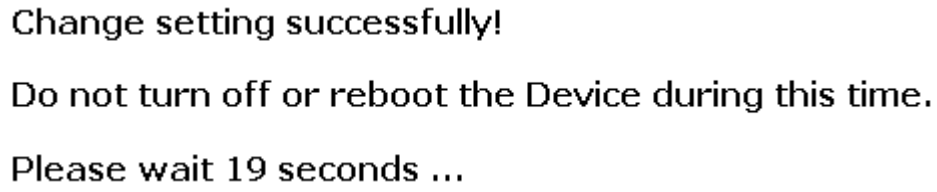
14. Selezionare l'opzione **Enable WDS**.
15. Digitare il **MAC Address** del peer AP
16. Digitare una descrizione nel campo **Comment**
17. Se è necessario configurare i parametri di sicurezza della rete, premere il pulsante **Set Security** ed impostare correttamente i relativi parametri.
18. Premere il pulsante **Apply Changes**


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
001333999980
Data Rate:
Auto
Comment:
001333999980
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

19. Premere il pulsante **Reboot Now**


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

20. Si visualizza il messaggio: *Le modifiche sono state correttamente effettuate! Non spegnere o riavviare il dispositivo. Attendere 20 secondi ...*



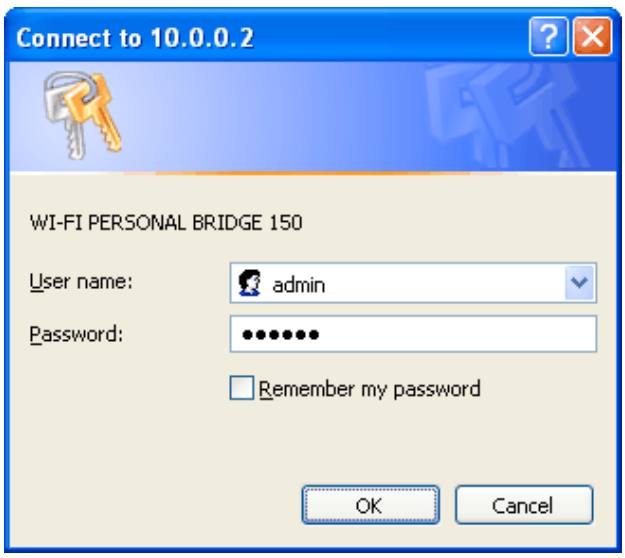
21. Premere " **Esci** " per terminare il programma.

22. In tal modo, il Router 802.11n Pocket AP e stato completamente configurato ed è pronto per permettere connessioni Wireless e connessioni ad Internet.

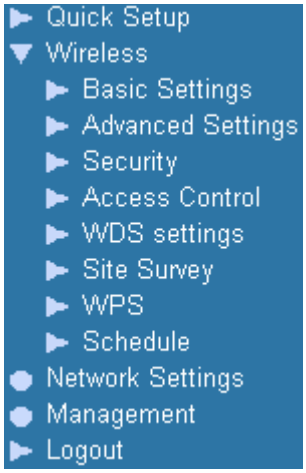
Configurazione avanzata per la modalità WiFi-AP Mode 3 – WDS + AP

1. Configurare sul PC un Adattatore Ethernet per avere un indirizzo IP fisso a 10.0.0.x (non utilizzare il valore 10.0.0.2).
2. Inserire il CD fornito nel lettore del PC.
3. Il CD si dovrebbe avviare automaticamente (modalità Auto-Start), visualizzando la schermata sottostante. Se il CD non si avvia automaticamente, aprire Risorse del Computer, selezionare il Driver del CD e quindi fare doppio click su "**autorun.exe**".
4. Per configurare il dispositivo, selezionare "**Advanced Configuration**".

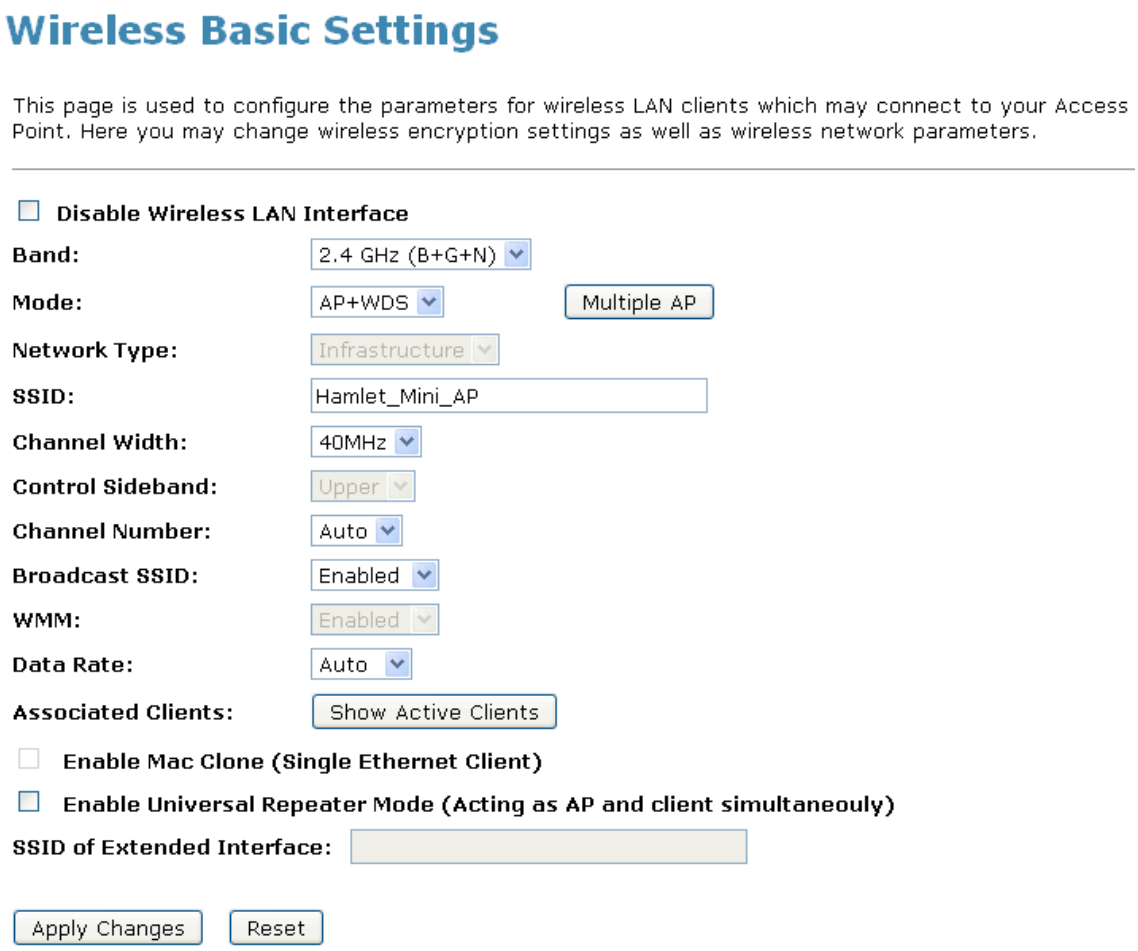
5. Nella finestra di Login digitare: User Name: **admin**, Password: **hamlet** e quindi confermare con il tasto **OK**.



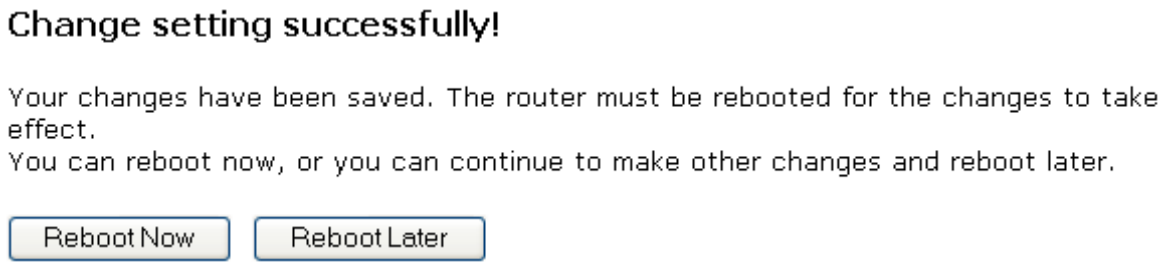
6. Selezionare il menù **Wireless -> Basic Settings**.



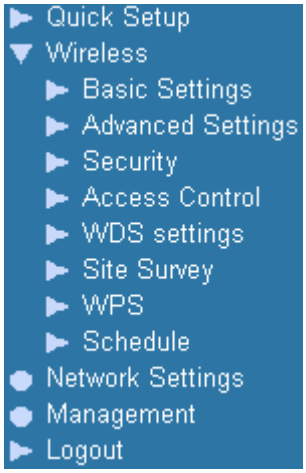
7. Selezionare **AP+WDS** dall'elenco del campo **Mode**
8. Impostare il valore per **Channel Width**
9. Impostare il valore per **Control Sideband**
10. Impostare il valore per **Channel Number**
11. Premere il pulsante **Apply Changes**



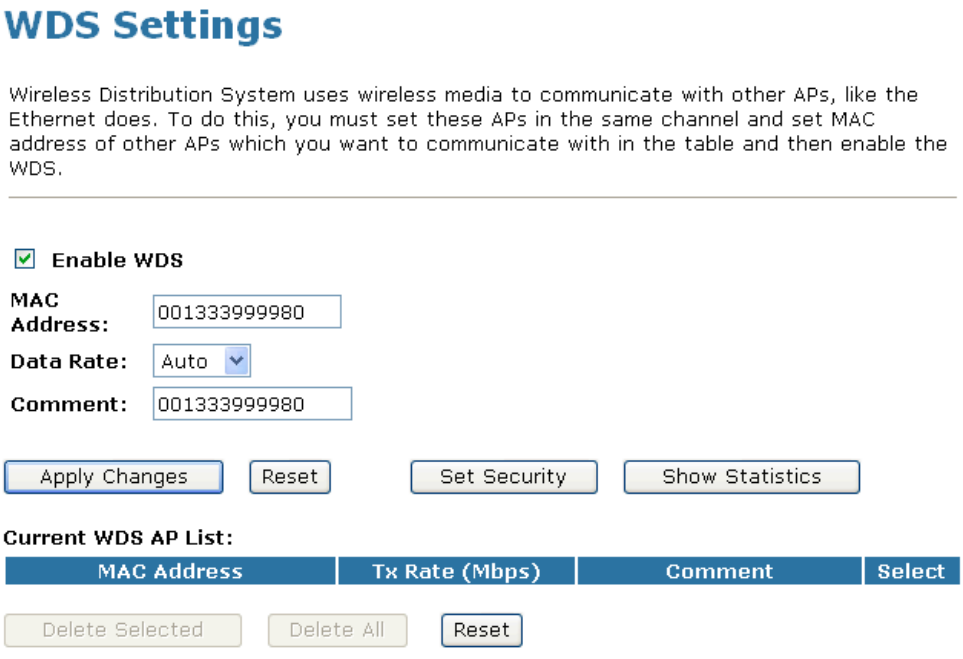
12. Premere il pulsante **Reboot Later**


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

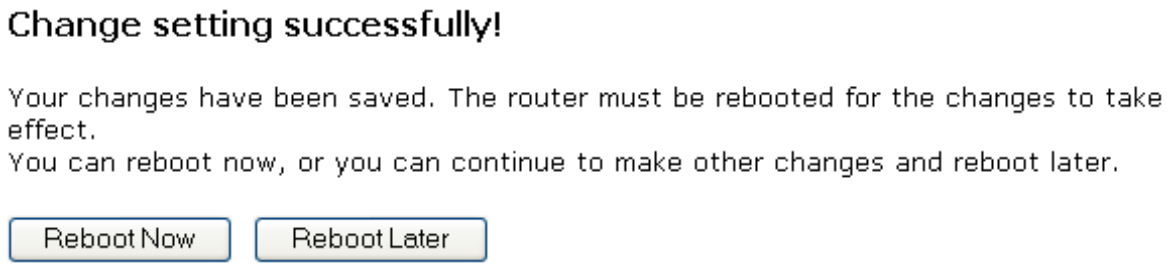
13. Selezionare il menù **Wireless -> WDS settings**.



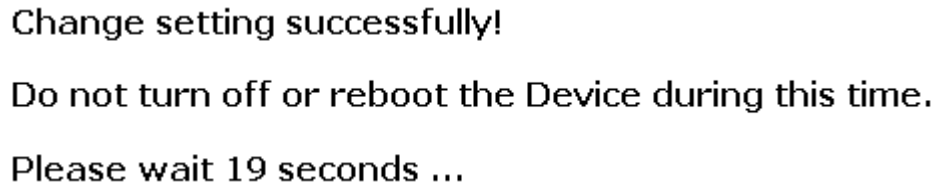
14. Selezionare l'opzione **Enable WDS**.
15. Digitare il MAC Address del peer AP
16. Digitare una descrizione nel campo Comment
17. Se è necessario configurare i parametri di sicurezza della rete, premere il pulsante **Set Security** ed impostare correttamente i relativi parametri.
18. Premere il pulsante **Apply Changes**


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
001333999980
Data Rate:
Auto
Comment:
001333999980
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

19. Premere il pulsante **Reboot Now**


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

20. Si visualizza il messaggio: *Le modifiche sono state correttamente effettuate! Non spegnere o riavviare il dispositivo. Attendere 20 secondi ...*



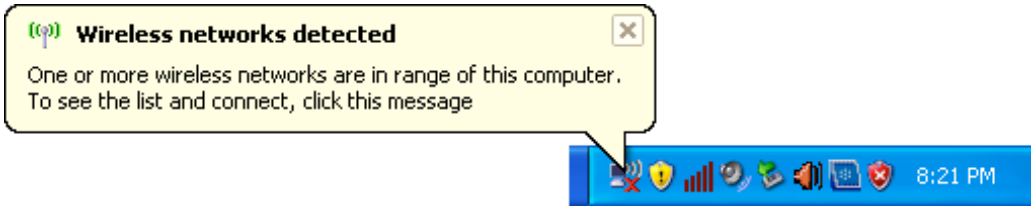
21. Premere " **Esci** " per terminare il programma.

22. In tal modo, il Router 802.11n Pocket AP e stato completamente configurato ed è pronto per permettere connessioni Wireless e connessioni ad Internet.

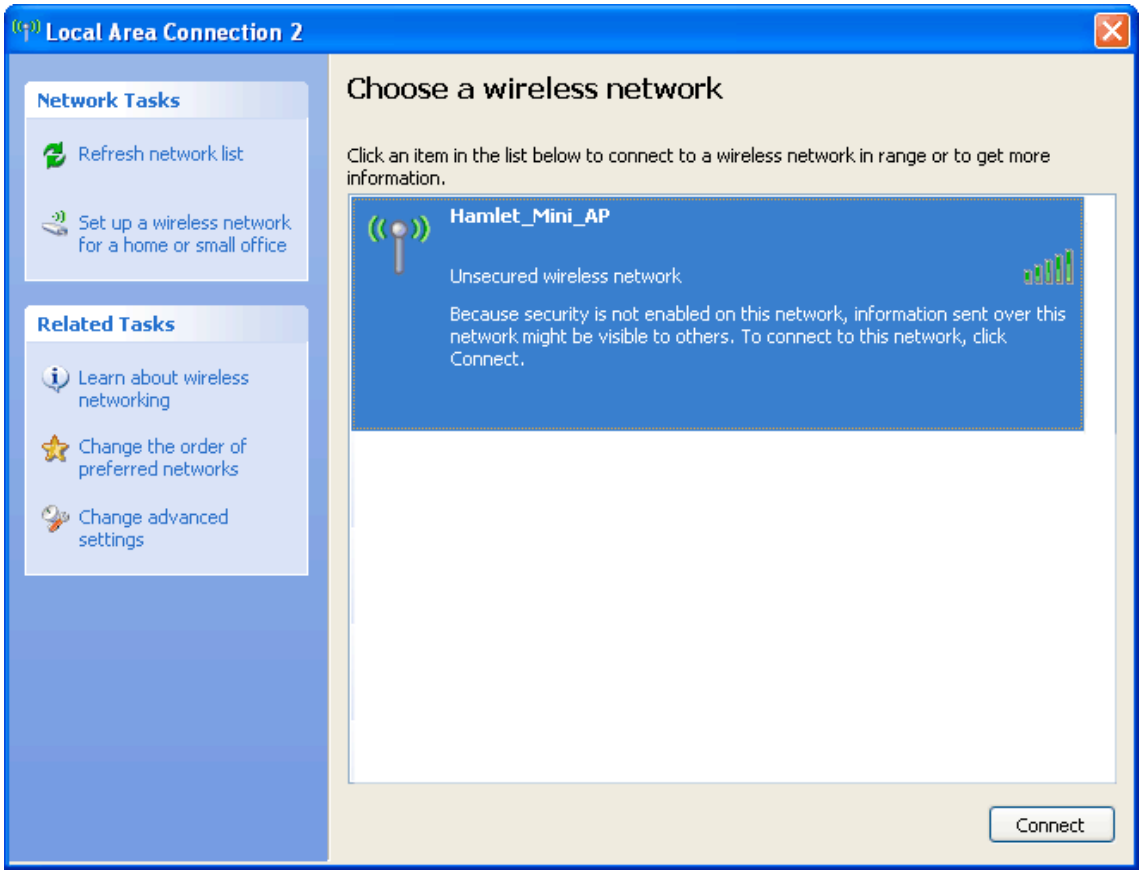
Connessione Wireless (solo per la modalità Router)

Per facilitare l'installazione si consiglia di salvare la configurazione. Successivamente si potrà modificare la configurazione mediante il menù di configurazione reti wireless. (si veda il manuale utente sul CD – Capitolo 9).

1. Fare un doppio click sull'icona della rete wireless sul computer e quindi ricercare la rete identificata dal nome **SSID**.


Wireless networks detected
One or more wireless networks are in range of this computer.
To see the list and connect, click this message
8:21 PM

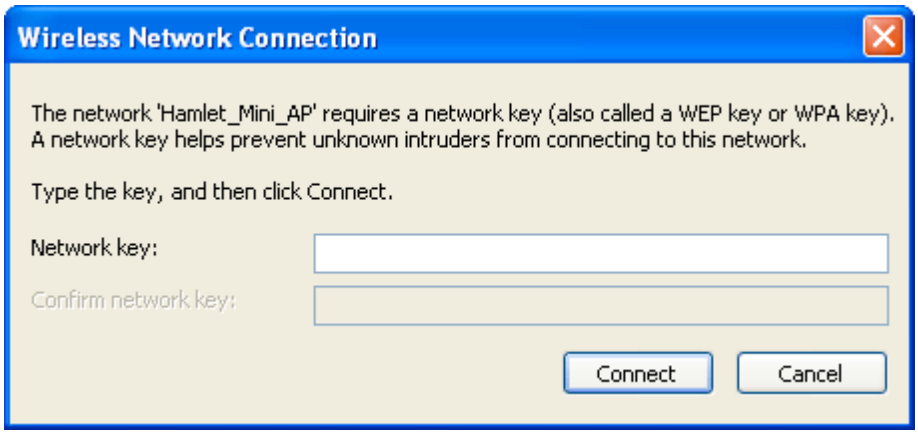
2. Selezionare la rete wireless con il nome **SSID** per collegarsi.


Local Area Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Hamlet_Mini_AP
Unsecured wireless network
Because security is not enabled on this network, information sent over this network might be visible to others. To connect to this network, click Connect.
Connect

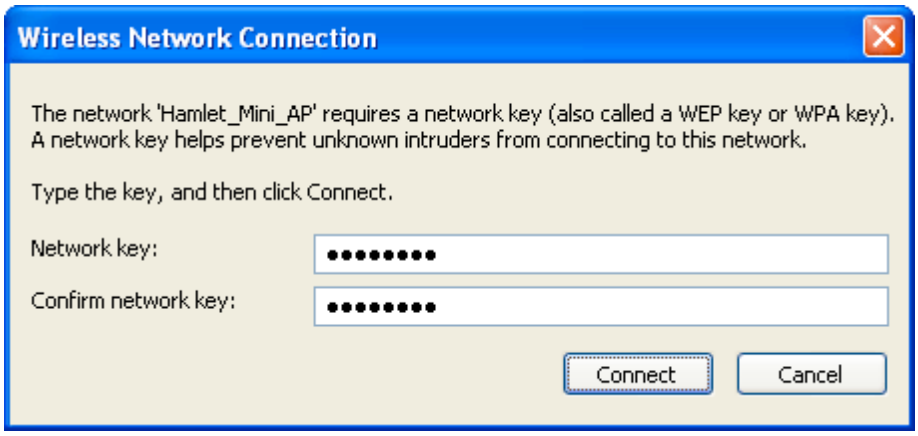
3. Se la rete wireless non è protetta, premere "**Connect Anyway**" per collegarsi.

Wireless Network Connection
You are connecting to the unsecured network "Hamlet_Mini_AP".
Information sent over this network is not encrypted and might be visible to other people.
Connect Anyway
Cancel

4. Se la rete wireless è protetta, digitare la chiave di rete che corrisponde a quella richiesta per l'autenticazione. Sarà possibile modificare successivamente tale chiave, mediante il menù di configurazione reti wireless. (si veda il manuale utente sul CD – Capitolo 9).


Wireless Network Connection
The network 'Hamlet_Mini_AP' requires a network key (also called a WEP key or WPA key).
A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

5. Premere "Connect" o "Apply".


Wireless Network Connection
The network 'Hamlet_Mini_AP' requires a network key (also called a WEP key or WPA key).
A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

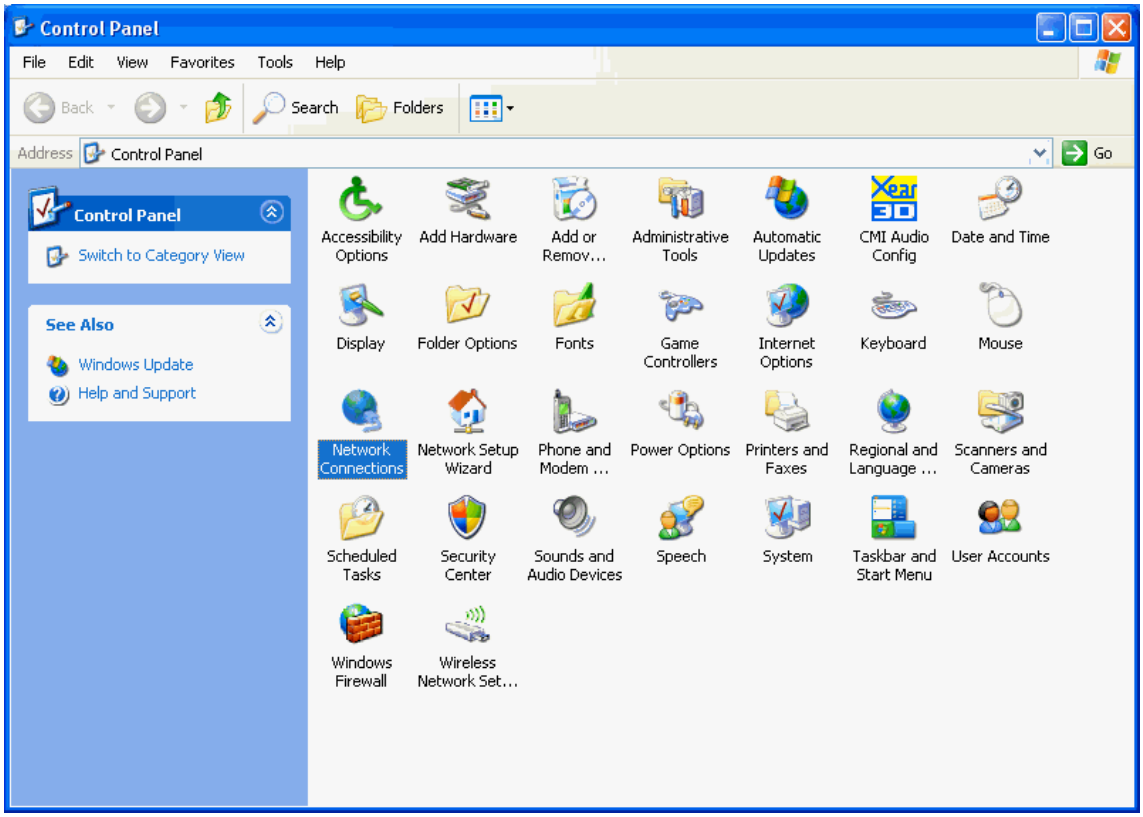
6. In tal modo si è pronti per utilizzare la rete Wireless per Internet o intranet.

6 Conoscere il tipo di accesso Internet/WAN disponibile

Prima di procedere con le restanti operazioni è necessario definire il tipo di accesso Internet/WAN disponibile, allo scopo di configurare opportunamente la porta WAN del Router.

Si consiglia di attenersi a quanto di seguito così da identificare la tipologia di accesso Internet/WAN: Client DHCP, IP statico o Client PPPoE.

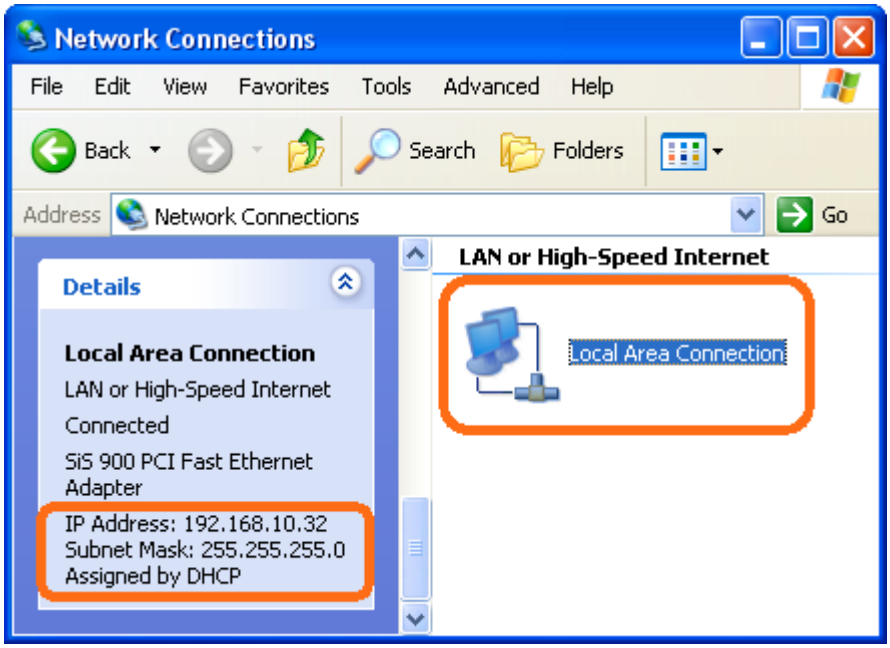
1. Fare click su Start -> Control Panel
2. Fare un doppio click su *Network Connections* (Connessioni di rete)



Accesso Internet/WAN di tipo Client DHCP

Se nella finestra delle connessioni di rete (**Network Connections**) non è presente alcun **Adattatore Broadband**, l'accesso Internet/WAN è di tipo **Client DHCP** o **IP statico**.

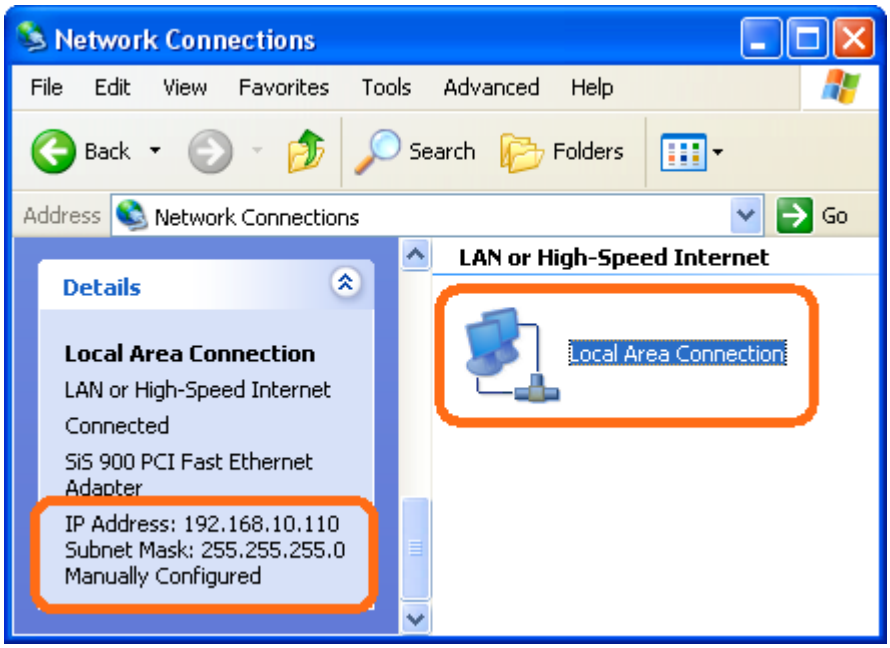
1. Fare click su **Local Area Connection** nella sezione **LAN or High-Speed Internet** e verificare che nel riquadro di sinistra, area Dettagli, si visualizzi l'indicazione **Assigned by DHCP**.



Accesso Internet/WAN di tipo IP statico

Se nella finestra delle connessioni di rete (**Network Connections**) non è presente alcun **Adattatore Broadband**, l'accesso Internet/WAN è di tipo **Client DHCP** o **IP statico**.

1. Fare click su **Local Area Connection** nella sezione **LAN or High-Speed Internet** e verificare che nel riquadro di sinistra, area Dettagli, si visualizzi l'indicazione **Manually Configured**.



2. Fare click con il tasto destro del mouse su **Local Area Connection** ad aprire le **Proprietà**. Dalla finestra delle Proprietà è possibile visualizzare la configurazione in dettaglio e quindi impostarla come segue:

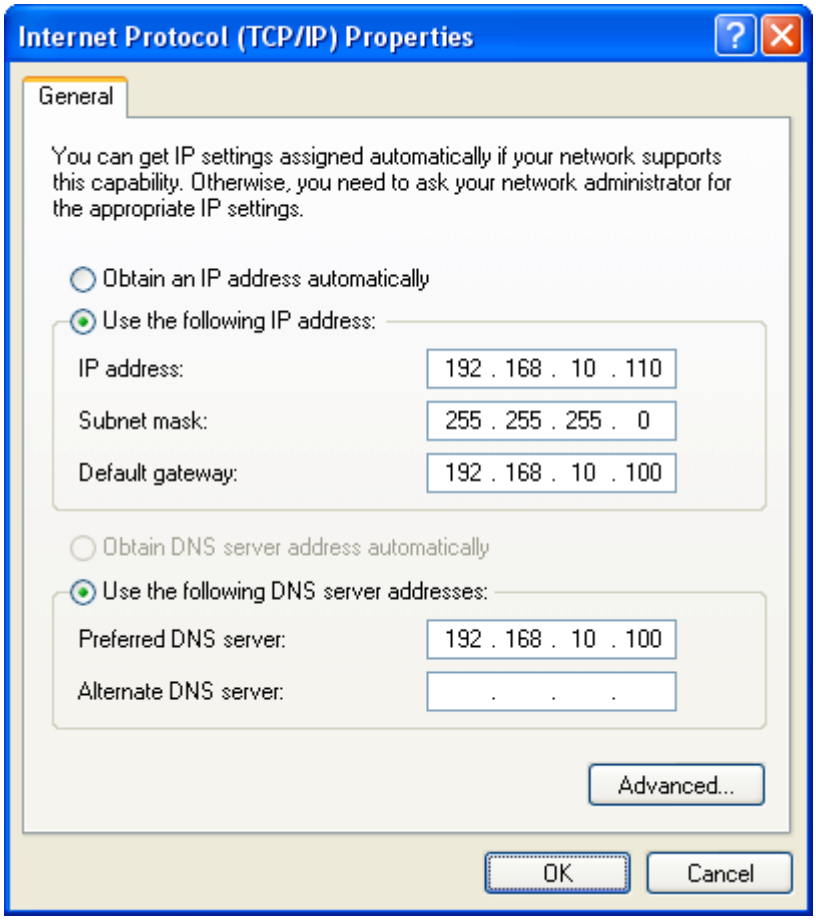
Indirizzo IP: 192.168.10.110

Subnet mask: 255.255.255.0

Default gateway: 192.168.10.100

Server DNS preferito: 192.168.10.100

Server DNS secondario: se si dispone tale informazione, inserirla nel campo relativo.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 10 . 110
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 10 . 100
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 10 . 100
Alternate DNS server:
Advanced...
OK
Cancel

Accesso Internet/WAN di tipo Client PPPoE

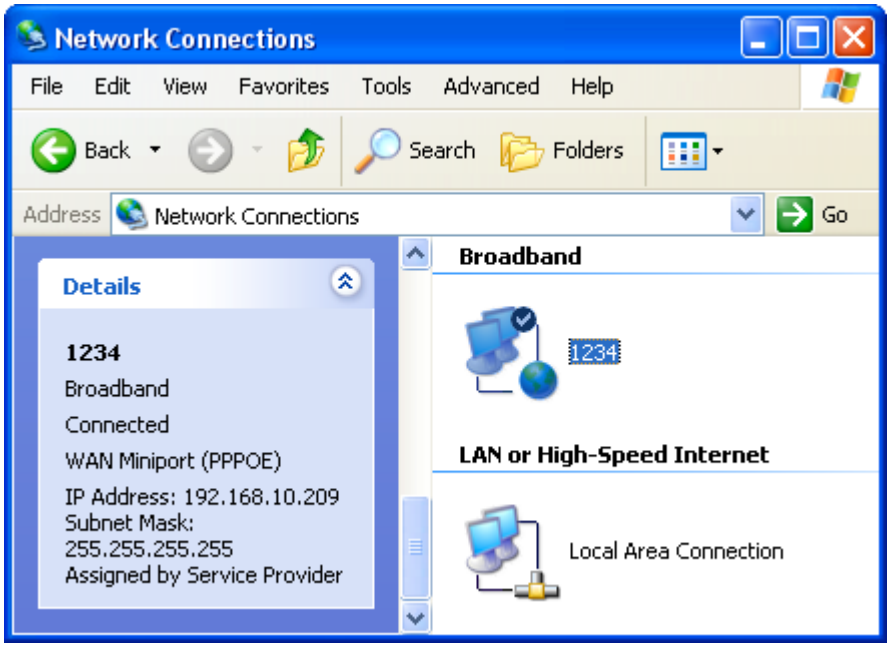
Se nella finestra delle connessioni di rete (**Network Connections**) è presente un **Adattatore Broadband**, l'accesso Internet/WAN è di tipo **Client PPPoE**.

1. Fare un click sul **Broadband Adapter** nella sezione **Broadband** e verificare che nel riquadro di sinistra, area Dettagli, si visualizzi l'indicazione **Assigned by Service Provider**.

Per la configurazione PPPoE sul Router è necessario seguire le informazioni fornite dalla Telecom o dall' Internet Service Provider.

Username PPPoE: 1234 (a titolo di esempio)

Password PPPoE: 1234 (a titolo di esempio)



7 Come utilizzare le pagine WEB

Il Router include una serie di pagine WEB da utilizzarsi per effettuare le procedure di installazione e configurazione dello stesso, così da ottimizzarlo per le esigenze specifiche della propria rete. L'accesso alle pagine WEB può essere effettuato mediante un qualunque browser del PC, collegandosi alla porta LAN del dispositivo.

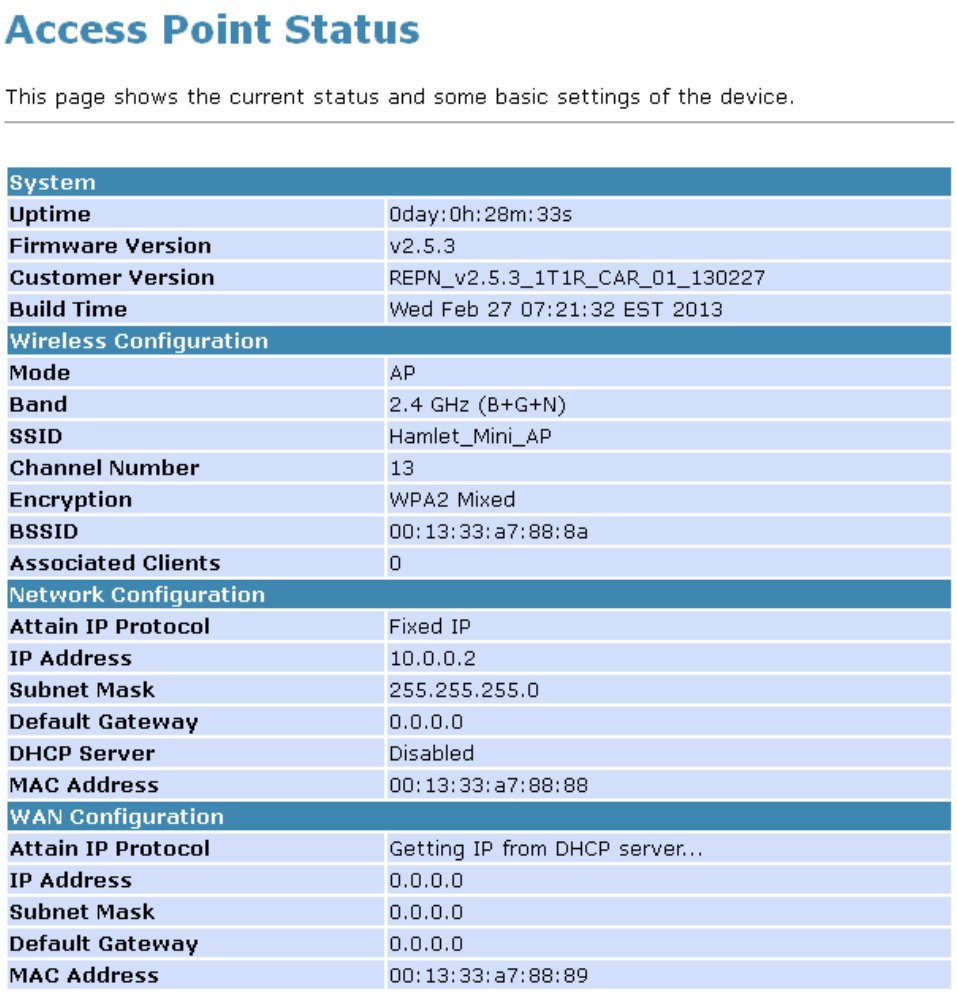
Accesso alle pagine Web

Per accedere alle pagine Web e necessario:

- un PC o un portatile collegato alla porta LAN del dispositivo.
- un browser installato sul PC. E' possibile utilizzare Internet Explorer 4 o Netscape 4 o qualsiasi versione successiva. Per la miglior qualità, si consiglia di utilizzare le ultime versioni di Internet Explorer, Netscape o Mozilla Firefox. Da qualsiasi computer connesso con il dispositivo via LAN, avviare il browser e digitare l'indirizzo IP del dispositivo:

  http://10.0.0.2

Confermando l'indirizzo digitato mediante il tasto invio, si visualizza la pagina di stato del dispositivo:



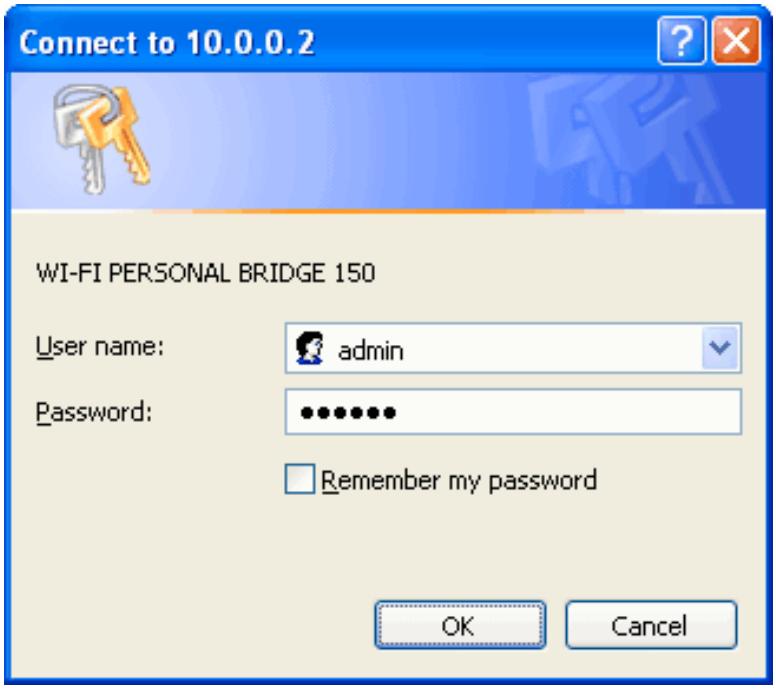
Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:28m:33s
Firmware Version	v2.5.3
Customer Version	REPN_v2.5.3_1T1R_CAR_01_130227
Build Time	Wed Feb 27 07:21:32 EST 2013
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	Hamlet_Mini_AP
Channel Number	13
Encryption	WPA2 Mixed
BSSID	00:13:33:a7:88:8a
Associated Clients	0
Network Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:13:33:a7:88:88
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:13:33:a7:88:89

La prima volta che si fa click (tasto sinistro del mouse) su uno dei valori visualizzati, si apre la finestra di login, in cui è necessario digitare username e password per accedere alle pagine di configurazione.

La pagina di login è mostrata di seguito:



1. Digitare username e password. Per il primo utilizzo è possibile effettuare il login con i seguenti valori di default:

User Name:	**admin**
Password:	**hamlet**

Nota

E' possibile cambiare la password in qualsiasi momento ovvero è possibile configurare il dispositivo in modo da non richiedere la password in fase di accesso. Si veda il paragrafo Password.

2. Confermare con OK. Effettuato il login si può procedere con la configurazione del dispositivo.

La pagina di login è visualizzata ogni qualvolta si acceda alle pagine WEB.

Nota

Se viene visualizzato un messaggio di errore o non si visualizza correttamente la pagina iniziale, far riferimento al paragrafo Risoluzione dei problemi

Verifica della configurazione

Dopo aver collegato il Router AP ed aver configurato i PC che sono connessi in LAN, da ciascun computer dovrebbe essere possibile usare la connessione DSL per accedere ad Internet.

Per effettuare il controllo della connessione, accendere il dispositivo, attendere 30 secondi e quindi verificare che i LED siano accesi come di seguito:

Tabella 1. Indicatori LED

Label	Color	Function
POWER	verde	ON: il dispositivo è acceso OFF: il dispositivo è spento
WLAN	verde	ON: collegamento WLAN attivo Lampeggio: scambio dati con rete WLAN
WPS	verde	OFF: collegamento WPS non attivo Lampeggio: scambio dati con rete WPS
WAN	verde	ON: collegamento WAN eseguito ed attivo OFF: assenza del collegamento WAN Lampeggio: scambio dati con rete WAN
LAN	verde	ON: collegamento LAN attivo OFF: assenza del collegamento LAN Lampeggio: scambio dati con rete LAN

Se i LED si accendono correttamente, effettuare una connessione da un computer in rete a scopo di test. A tale scopo, aprire il Browser e digitare l'indirizzo di un qualsiasi sito Internet (ad esempio http://www.yahoo.com). Il LED denominato WAN dovrebbe lampeggiare velocemente e quindi rimanere accesso fisso quando si è stabilita la connessione con il sito.

Se il LED non si illumina come dovrebbe, è necessario verificare che i parametri di configurazione della connessione corrispondano ai dati forniti dal proprio ISP (Internet Service Provider). Per ulteriori dettagli si veda il paragrafo *Accesso ad Internet*. Se dopo aver verificato i dati i LED continuano a non accendersi correttamente, far riferimento al paragrafo *Risoluzione dei problemi* o contattare l'assistenza del proprio ISP.

Configurazione di default del dispositivo

Per gestire al meglio la connessione xDSL / Modem di linea all'ISP, il Router fornisce una serie di funzionalità e di servizi specifici. Il dispositivo è preconfigurato con dei parametri di default per un utilizzo in reti domestiche o per piccole reti aziendale.

La tebella seguente elenca alcuni dei principali parametri di default; questi ed altri parametri sono completamente descritti nei successivi capitoli. Se si è esperti nella configurazione delle reti, riverificare ed in caso modificare i parametri predefiniti al fine di ottimizzare la configurazione con la propria rete. Seguire le istruzioni fornite per modificare tali valori, se necessario. Se non si è esperti, si consiglia di provare ad utilizzare il dispositivo senza modificare i parametri predefiniti oppure di contattare il proprio ISP per assistenza.

ATTENZIONE

Si consiglia vivamente di contattare il proprio ISP prima di modificare i valori di default.

Opzione	Valore di default	Descrizione/Istruzioni
Indirizzo IP lato WAN	DHCP Client	E' l'indirizzo IP pubblico assegnato temporaneamente dal lato della rete WAN del dispositivo. Rappresenta un valore fittizio che sarà sostituito dall' ISP non appena verrà assegnato l'indirizzo IP definitivo. Si veda *Network Settings -> WAN Interface*.
Indirizzo IP lato LAN	Indirizzo IP statico assegnato: 10.0.0.2 Subnet mask: 255.255.255.0	E' l'indirizzo IP definito dal lato della porta LAN del dispositivo. Tale porta si utilizza per collegare il dispositivo alla vostra rete Ethernet. Tipicamente non si dovrebbe cambiare questo indirizzo. Si veda *Network Settings -> LAN Interface*.
DHCP (Dynamic Host Configuration Protocol)	DHCP server abilitato con il seguente gruppo di indirizzi: 10.0.0.100 fino a 10.0.0.200	Il Gateway Wireless mantiene un gruppo di indirizzi IP privati per l'assegnamento dinamico degli indirizzi IP ai computer della rete LAN. Allo scopo di utilizzare questo servizio, si deve configurare i computer per accettare l'assegnazione dinamica degli indirizzi IP, come descritto nel capitolo *Configurazione IP automatico.*

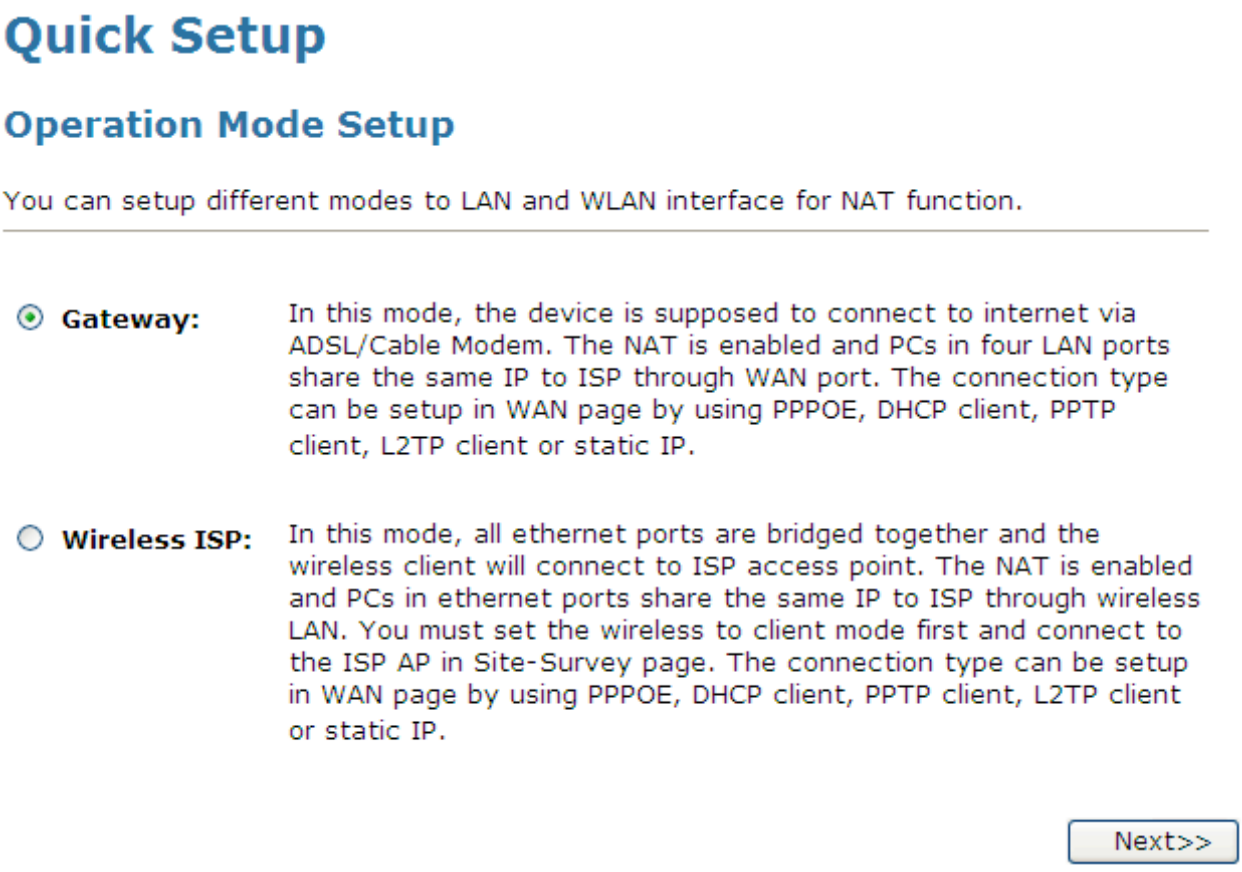
8 Setup rapido (la funzione può variare in funzione della modalità Router, Client o WiFi-AP)

La schermata di Setup Rapido visualizza informazioni utili circa la configurazione del dispositivo, relativamente alle seguenti funzioni:

- accesso ad Internet
- funzione VoIP
- modalità Wireless

Per visualizzare questa pagina:

Dal menù di sinistra selezionare *Quick Setup*. Si visualizza la seguente pagina:


Quick Setup
Operation Mode Setup
You can setup different modes to LAN and WLAN interface for NAT function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Next>>

Configurazione della modalità operativa

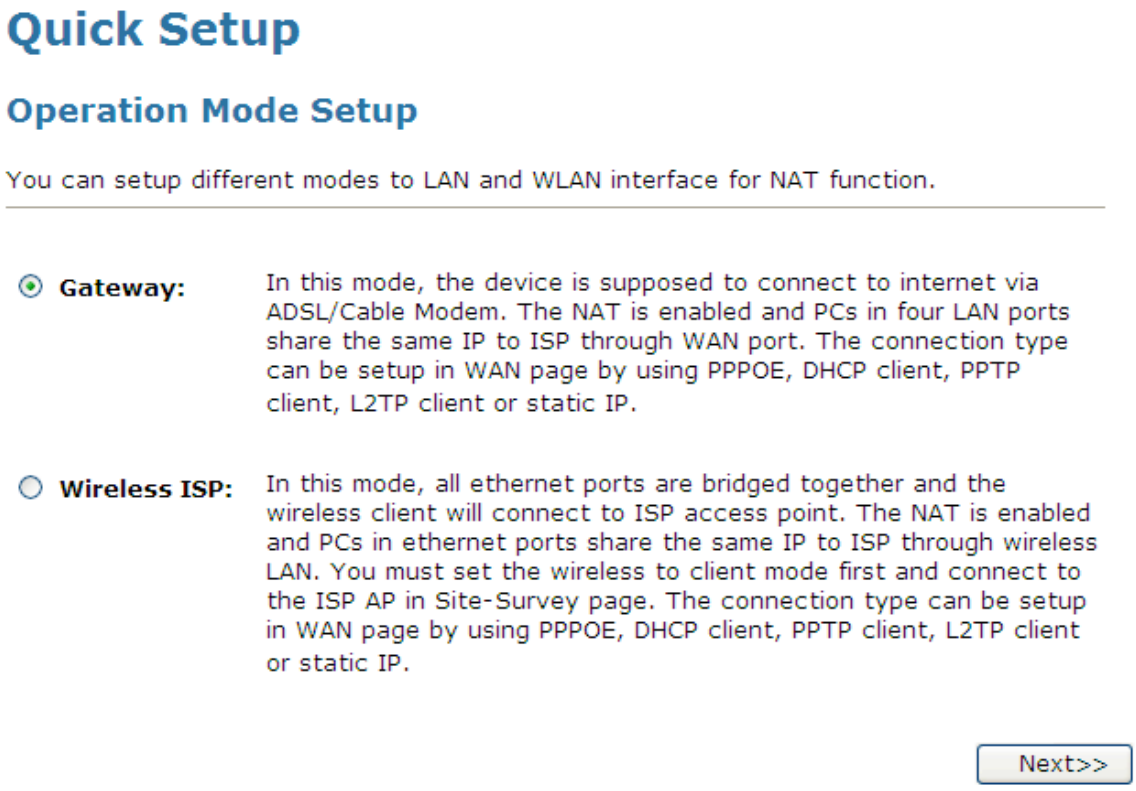
E' possibile selezionare differenti modalità operative per la funzione NAT delle interfacce LAN e WLAN.

Gateway

In questa modalità, si suppone che il dispositivo sia collegato ad Internet via ADSL/Modem di linea. La funzione NAT è abilitata ed i PC collegati alle porte LAN condividono lo stesso indirizzo IP assegnato dall'ISP per la porta WAN. Il tipo di connessione può essere configurata nella pagina di setup della funzione WAN, selezionando PPPoE, Client DHCP o IP statico.

Per cambiare la modalità operativa:

1. Dal menù di sinistra selezionare *Quick Setup*. Si visualizza la seguente pagina:
2. Selezionare l'opzione *Gateway* e quindi premere *Next>>*.

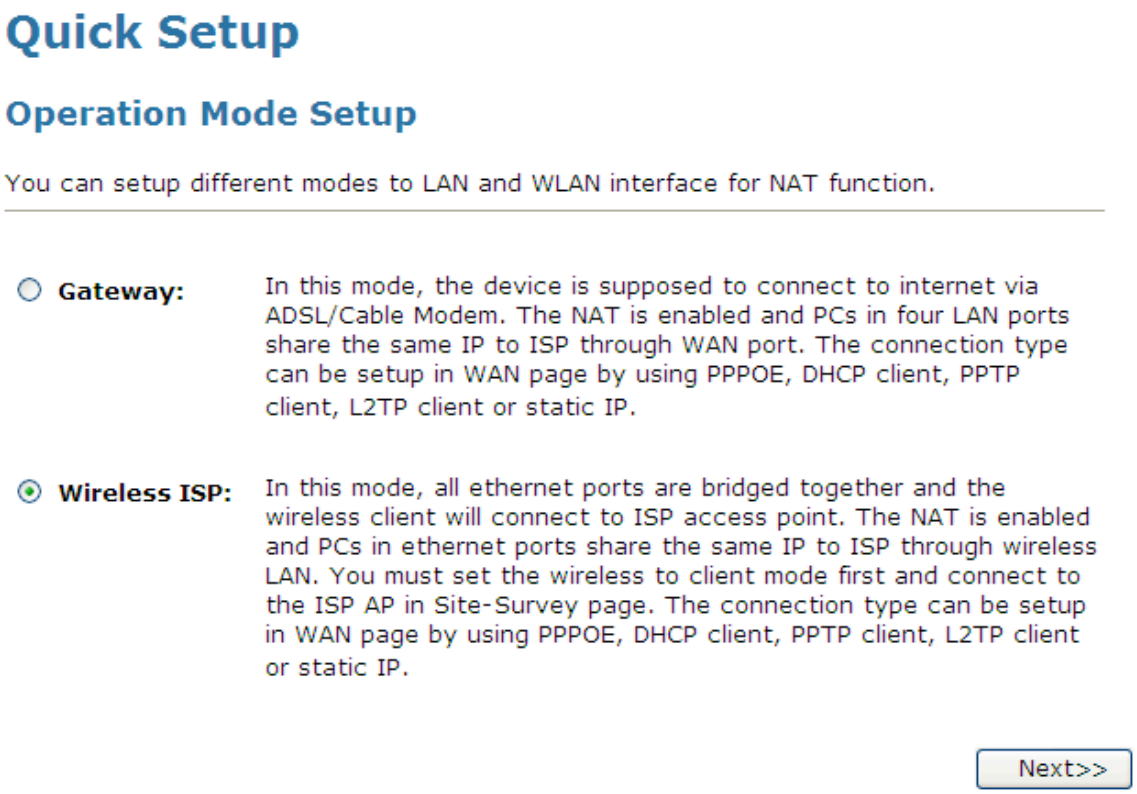

Quick Setup
Operation Mode Setup
You can setup different modes to LAN and WLAN interface for NAT function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Next>>

Wireless ISP

In questa modalità, tutte le porte Ethernet sono in bridge tra loro e il client della rete wireless si collega mediante accesso ISP. La funzione NAT è abilitata ed i PC collegati alle porte Ethernet condividono lo stesso indirizzo IP assegnato dall'ISP per la porta wireless LAN. E' necessario impostare prima la wireless come modalità Client e quindi collegarsi all' ISP AP dalla pagina Site-Survey. Il tipo di connessione può essere configurata nella pagina WAN, selezionando PPPOE, Client DHCP o IP statico.

Per cambiare la modalità operativa:

1. Dal menù di sinistra selezionare *Quick Setup*. Si visualizza la seguente pagina:
2. Selezionare l'opzione *Wireless ISP* e quindi premere *Next*>>.

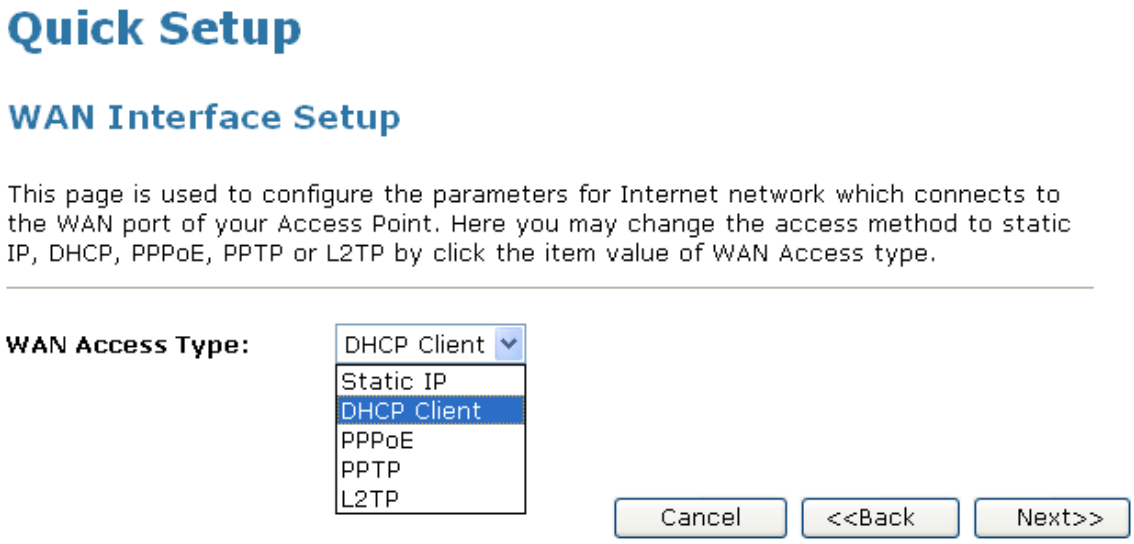

Quick Setup
Operation Mode Setup
You can setup different modes to LAN and WLAN interface for NAT function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Next>>

Configurazione della Interfaccia WAN

Questa pagina si utilizza per configurare i parametri della rete Internet connessa alla porta WAN del dispositivo. Da questa pagina si può modificare il metodo di accesso ad internet come IP statico, DHCP, PPPoE, PPTP o L2TP, selezionando il valore del tipo di accesso.

Per modificare il tipo di Accesso WAN:

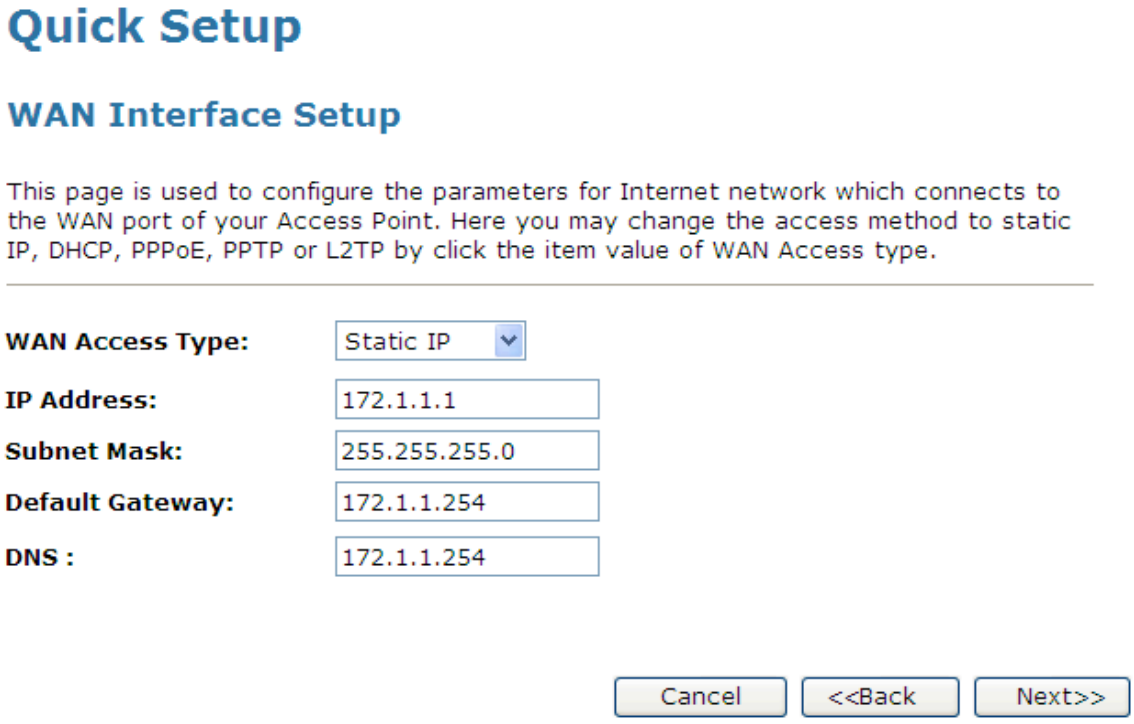
1. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *Static IP*, *DHCP Client*, *PPPoE*, *PPTP* o *L2TP* in funzione di quanto indicato dall'amministratore di rete o dall' ISP.
2. Premere il pulsante *Next>>*.


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Static IP
DHCP Client
PPPoE
PPTP
L2TP
Cancel
<<Back
Next>>

Static IP

In questa modalità, si suppone che il dispositivo sia collegato ad Internet via ADSL o Modem di linea. La funzione NAT è abilitata ed i PC collegati alle porte LAN condividono lo stesso indirizzo IP assegnato dall'ISP per la porta WAN. Il tipo di connessione può essere configurata nella pagina di setup della funzione WAN, selezionando Static IP.

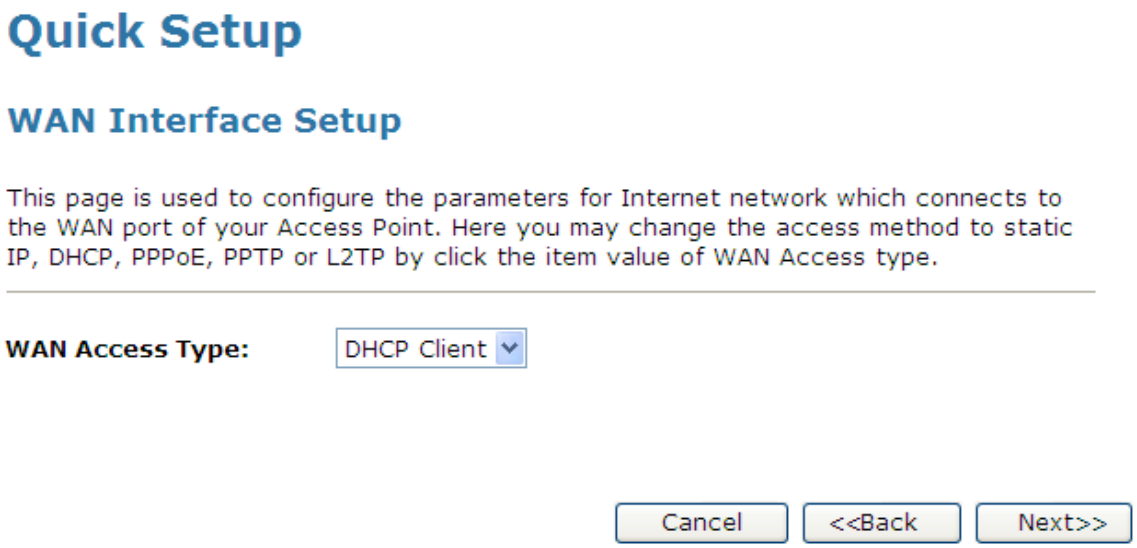
1. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *Static IP* in funzione di quanto indicato dall'amministratore di rete o dall' ISP.
2. Digitare l'indirizzo IP (*IP Address*) (ad esempio 172.1.1.1).
3. Digitare la *Subnet Mask* (ad esempio 255.255.255.0).
4. Digitare l'indirizzo del *Default Gateway* (ad esempio 172.1.1.254).
5. Digitare l'indirizzo *DNS* (ad esempio 172.1.1.254).
6. Premere il pulsante *Next>>*.


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
Static IP
IP Address:
172.1.1.1
Subnet Mask:
255.255.255.0
Default Gateway:
172.1.1.254
DNS :
172.1.1.254
Cancel
<<Back
Next>>

DHCP Client

In questa modalità, si suppone che il dispositivo sia collegato ad Internet via ADSL o Modem di linea. La funzione NAT è abilitata ed i PC collegati alle porte LAN condividono lo stesso indirizzo IP assegnato dall'ISP per la porta WAN. Il tipo di connessione può essere configurata nella pagina di setup della funzione WAN, selezionando Static IP.

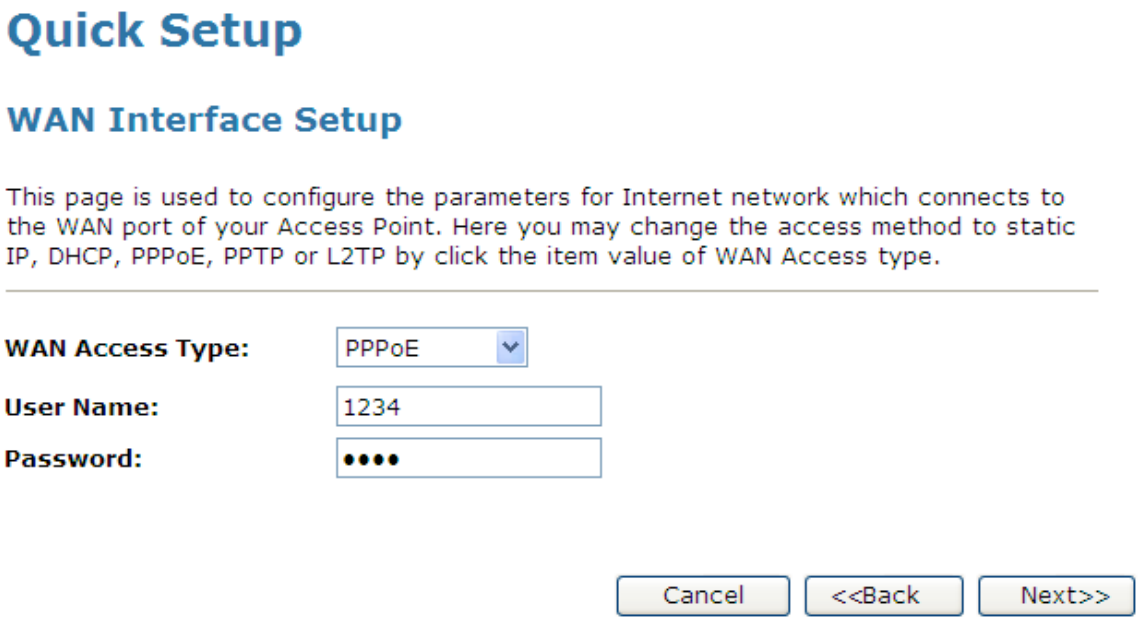
1. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *DHCP* in funzione di quanto indicato dall'amministratore di rete o dall' ISP.
2. Premere il pulsante *Next>>*.


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Cancel
<<Back
Next>>

PPPoE

In questa modalità, si suppone che il dispositivo sia collegato ad Internet via ADSL o Modem di linea. La funzione NAT è abilitata ed i PC collegati alle porte LAN condividono lo stesso indirizzo IP assegnato dall'ISP per la porta WAN. Il tipo di connessione può essere configurata nella pagina di setup della funzione WAN, selezionando Static IP.

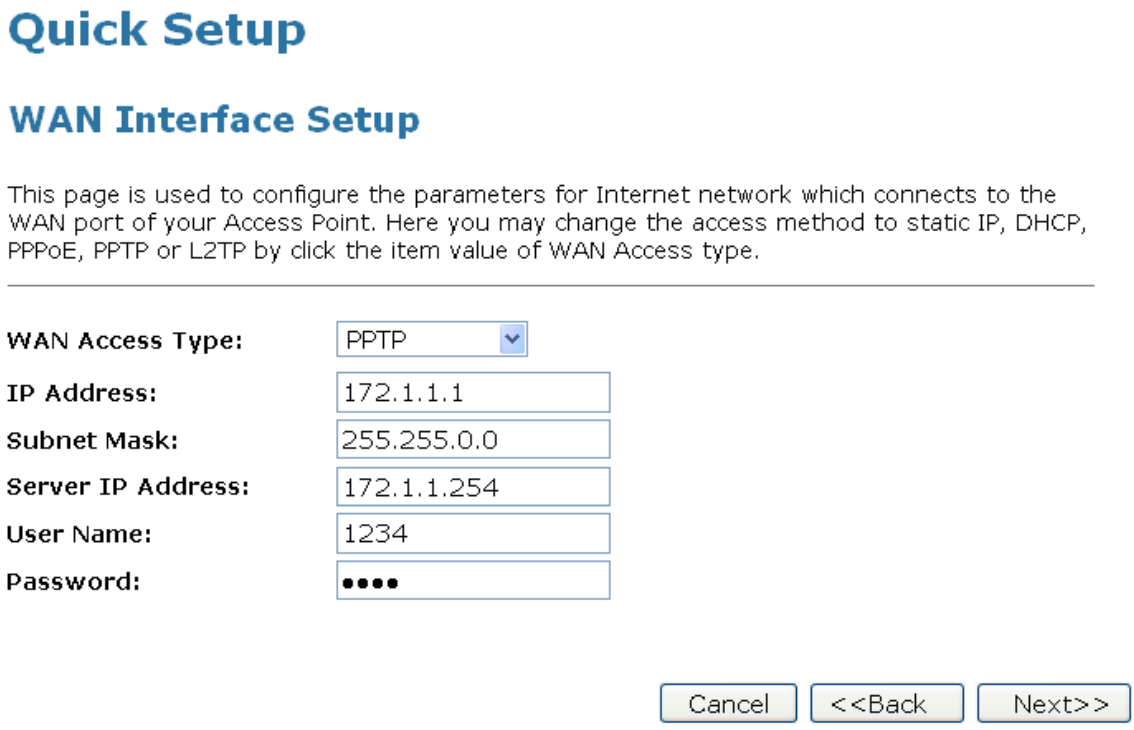
1. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *PPPoE* in funzione di quanto indicato dall'amministratore di rete o dall' ISP.
2. Digitare lo *User Name* (ad esempio 1234).
3. Digitare la *Password* (ad esempio 1234).
4. Premere il pulsante *Next>>*.


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
PPPoE
User Name:
1234
Password:
Cancel
<<Back
Next>>

PPTP

In questa modalità, si suppone che il dispositivo sia collegato ad Internet via ADSL o Modem di linea. La funzione NAT è abilitata ed i PC collegati alle porte LAN condividono lo stesso indirizzo IP assegnato dall'ISP per la porta WAN. Il tipo di connessione può essere configurata nella pagina di setup della funzione WAN, selezionando Static IP.

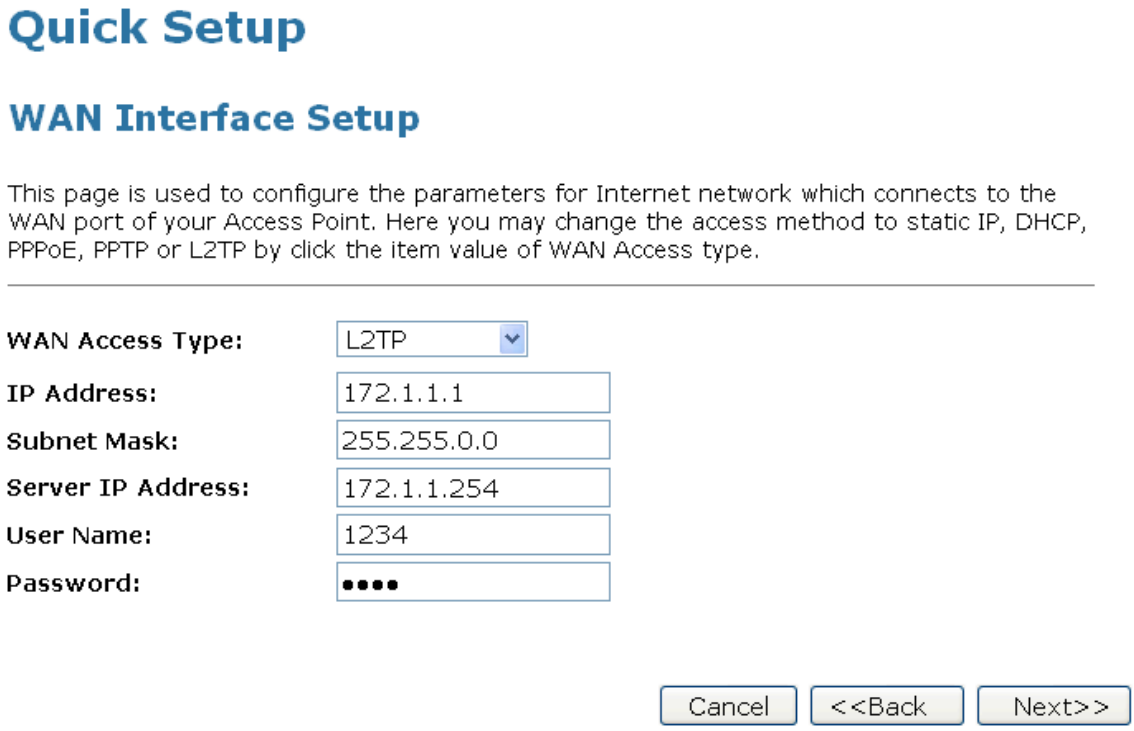
1. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *PPTP* in funzione di quanto indicato dall'amministratore di rete o dall' ISP.
2. Digitare l'indirizzo IP (*IP Address*) (ad esempio 172.1.1.1) fornito dall'Amministratore di rete o dall' ISP.
3. Digitare la *Subnet Mask* (ad esempio 255.255.0.0) fornita dall'Amministratore di rete o dall' ISP.
4. Digitare l'indirizzo *Server IP Address* (ad esempio 172.1.1.254) fornito dall'Amministratore di rete o dall' ISP.
5. Digitare lo *User Name* (ad esempio 1234) fornito dall'Amministratore di rete o dall' ISP.
6. Digitare la *Password* (ad esempio 1234) fornito dall'Amministratore di rete o dall' ISP.
7. Premere il pulsante *Next>>*.


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
PPTP
IP Address:
172.1.1.1
Subnet Mask:
255.255.0.0
Server IP Address:
172.1.1.254
User Name:
1234
Password:
Cancel
<<Back
Next>>

L2TP

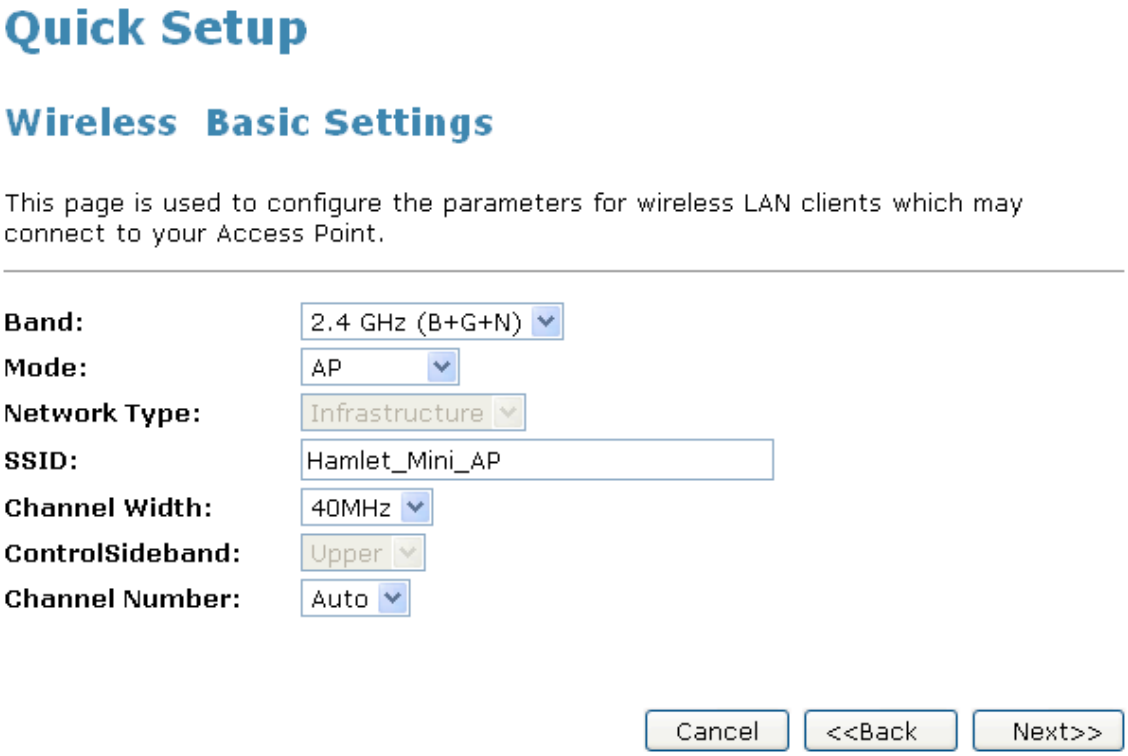
In questa modalità, si suppone che il dispositivo sia collegato ad Internet via ADSL o Modem di linea. La funzione NAT è abilitata ed i PC collegati alle porte LAN condividono lo stesso indirizzo IP assegnato dall'ISP per la porta WAN. Il tipo di connessione può essere configurata nella pagina di setup della funzione WAN, selezionando Static IP.

1. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *L2TP* in funzione di quanto indicato dall'amministratore di rete o dall' ISP.
2. Digitare l'indirizzo IP (*IP Address*) (ad esempio 172.1.1.1) fornito dall'Amministratore di rete o dall' ISP.
3. Digitare la *Subnet Mask* (ad esempio 255.255.0.0) fornita dall'Amministratore di rete o dall' ISP.
4. Digitare l'indirizzo *Server IP Address* (ad esempio 172.1.1.254) fornito dall'Amministratore di rete o dall' ISP.
5. Digitare lo *Username* (ad esempio 1234) fornito dall'Amministratore di rete o dall' ISP.§
6. Digitare la *Password* (ad esempio 1234) fornito dall'Amministratore di rete o dall' ISP.
7. Premere il pulsante *Next>>*.


Quick Setup
WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
L2TP
IP Address:
172.1.1.1
Subnet Mask:
255.255.0.0
Server IP Address:
172.1.1.254
User Name:
1234
Password:
Cancel
<<Back
Next>>

Configurazione di base della rete Wireless

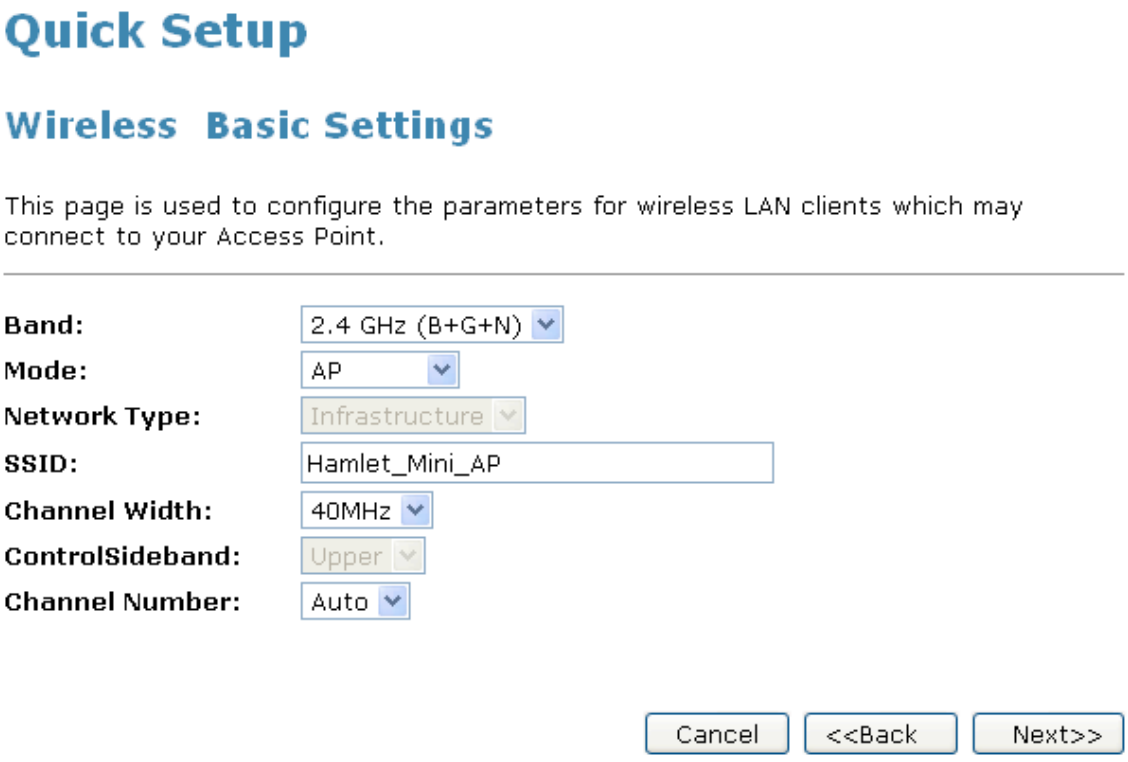
Questa pagina permette di configurare i parametri della rete Wireless necessari per il collegamento dei Client all'Access Point.



AP (Access Point)

Questa pagina permette di configurare i parametri necessari affinché i Client della rete Wireless possano collegarsi all'Access Point.

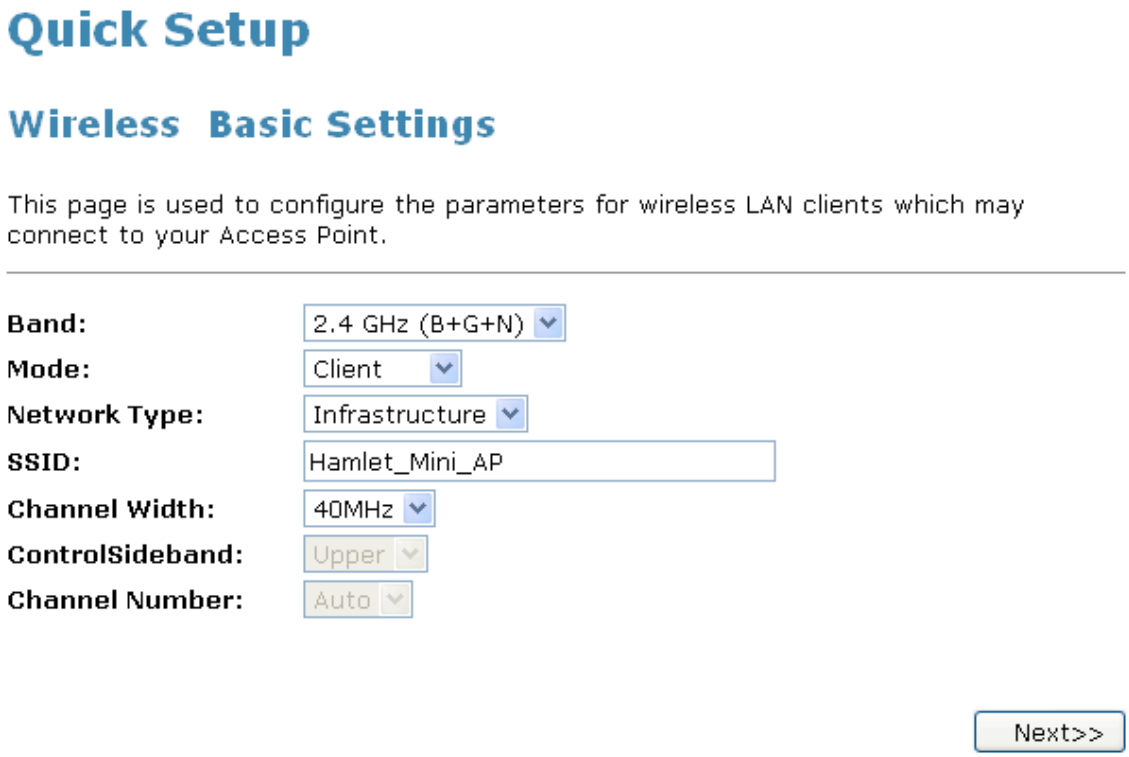
1. Selezionare dall'elenco del campo *Band* un valore di Banda opportuno.
2. Selezionare dall'elenco del campo *Mode* l'opzione *AP*.
3. Digitare l'*SSID* di rete (ad esempio 11n Pocket AP).
4. Selezionare dall'elenco del campo *Channel Width* un valore opportuno per la larghezza di banda del canale.
5. Selezionare dall'elenco del campo *Control SideBand* un valore opportuno.
6. Selezionare dall'elenco del campo *Channel Number* il numero da assegnare al canale.
7. Premere il pulsante *Next>>*.



Client

Questa pagina permette di configurare i parametri per la connessione dei Client della rete Wireless che potrebbero collegarsi all'Access Point.

1. Selezionare dall'elenco del campo *Band* un valore di Banda opportuno.
2. Selezionare dall'elenco del campo Mode l'opzione *Client*.
3. Selezionare dall'elenco del campo *Network Type* un tipo di rete.
4. Digitare l'*SSID* di rete (ad esempio 11n Pocket AP).
5. Premere il pulsante *Next>>*.



WDS (Wireless Distribution System)

WDS è l'acronimo di Wireless Distribution System (Sistema Distribuito Wireless) e permette di abilitare i punti di accesso della rete, denominati Access Point (AP), a collegarsi in modalità Wireless. Il servizio WDS può essere fornito anche da dispositivi di tipo Integrated Access Device.

Nota

Apparati di tipo Integrated Access Device che supportano il WDS, non supportano però sistemi di sicurezza delle reti WDS quali WEP, WPA o WPA-Enterprise.

Qualche volta può essere necessario realizzare una rete Wireless in casa o in ufficio in cui siano presenti più Access Point, trovandosi però nella condizione che non siano disponibili le connessioni Ethernet via cavo nei punti in cui si vogliono posizionare i vari Access Point. In fin dei conti, potrebbe essere necessario l'utilizzo di una rete Wireless proprio perchè non si dispone dei cavi Ethernet cablati nell'impianto dei locali della rete.

Una delle soluzioni a questo problema è quella di utilizzare un sistema composto da più Gateway Wireless, conosciuto anche come Wireless Distribution System (WDS).

Fondamentalmente, la tecnica WDS crea una porzione di rete fornendo i meccanismi per far 'parlare' gli Access Point tra di loro, così come inviare i dati ai dispositivi associati agli Access Point.

Nota

Il WDS è un sistema basato su alcuni protocolli standard 802.11, ma allo stato attuale non è stato ancora definito uno standard preciso su come debbano interagire Access Point e Router di differenti costruttori. Per questo motivo, avendo un Gateway Wireless in una posizione fisica e volendo espandere la rete con un Router di altro tipo e di un altro costruttore, potrebbero verificarsi dei malfunzionamenti. Si ha maggior fortuna se si utilizzano apparati dello stesso costruttore.

Nota

Quando si usa un WDS come sistema ripetitore, così come descritto di seguito, si dimezza la velocità per i Client connessi ad un Integrated Wireless Gateway. Questo perchè ciascun bit di dati deve necessariamente essere inviato due volte (i dati sono ricevuti dall'Access Point e quindi ritrasmessi).

Per configurare il WDS, è necessario modificare alcuni parametri di configurazione su ciascun AP della rete. Le operazioni da effettuare (così come la terminologia utilizzata) può variare da costruttore a costruttore. In generale, si dovrebbero comunque trovare delle configurazioni tipo quelle di seguito descritte.

Postazione WDS principale:

Una della postazioni WDS è la postazione principale della rete WDS. Questa AP è connessa direttamente alla connessione Internet ovvero è connessa al router mediante un collegamento via cavo. La stazione principale è il bridge per la connessione Internet su cui può passare tutto il traffico wireless.

Postazione WDS ripetitore:

In una rete composta semplicemente da due AP WDS, l'AP "non collegato via cavo" è un ripetitore. Il ripetitore riceve i dati dalla postazione principale (o postazione base) e reinvia i dati ai Client wireless che sono associati alla postazione ripetitore (e viceversa per i dati provenienti dai Client).

Se nella rete sono presenti più di due AP, le AP remote possono operare come ripetitori oppure potrebbero operare come punto di interruzione dei dati, se il ripetitore è troppo distante dalla postazione principale per comunicare.

Quando si configura la postazione WDS principale o base, è importante annotarsi il canale che è stato configurato per l'utilizzo e l' SSID o il nome di rete assegnato alla propria rete WDS. E' importante verificare che l' AP non abbia attive funzionalità di auto configurazione che selezionano il canale base in modo automatico in funzione delle condizioni della rete; in caso contrario assicurarsi che tali funzionalità siano disabilitate. Se la stazione WDS principale svolge anche funzione di Router di rete, assicurarsi che siano anche impostate le funzionalità di assegnazione degli indirizzi IP ai dispositivi presenti in rete.

Nota

Trascrivere o comunque annotarsi gli indirizzi MAC di tutte le postazioni WDS — molti sistemi software di configurazione richiedono tali indirizzi per poter configurare correttamente il sistema. Prestare attenzione nell'annotarsi l'indirizzo MAC della interfaccia wireless (spesso riportata su un'etichetta) e non l'indirizzo MAC della interfaccia Ethernet.

Attivare la funzionalità WDS sulla postazione principale (è spesso chiamata WDS ma si può anche essere identificata come WDS Main Base Station — tipicamente è il modo che utilizza Apple per i prodotti AirPort Extreme). Quando si attiva la funzionalità WDS, il software di configurazione potrebbe richiedere di identificare il o i ripetitori remoti. In questo caso può essere necessario avere a portata di mano gli indirizzi MAC dei ripetitori.

In base a come opera il software, potrebbe essere necessario accedere direttamente al software di configurazione dei ripetitori AP per attivare la funzionalità WDS.

Di seguito si riportano alcune annotazioni da tenere presenti:

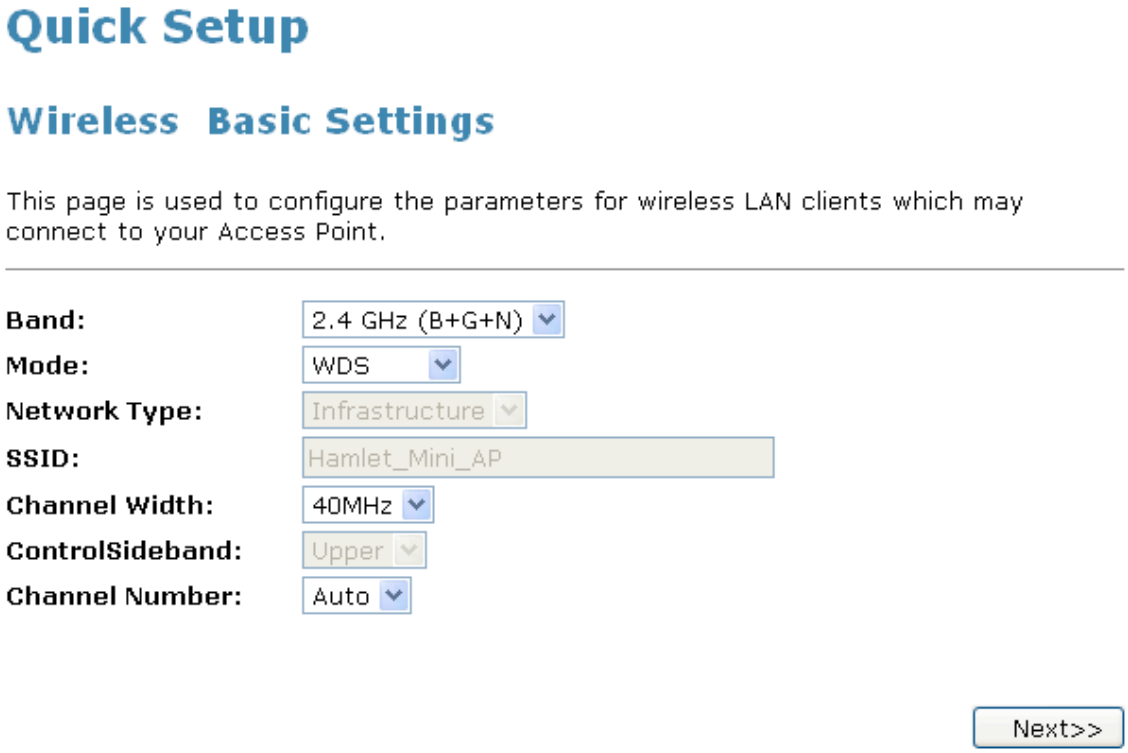
- Si deve assegnare ogni altra postazione WDS sullo stesso canale che è stato assegnato alla postazione WDS base. Questo potrebbe non essere così intuitivo per molte persone che per lungo tempo si sono sempre attenute alla "linea guida" di configurazione delle reti a standard 802.11b/g per cui era necessario "usare i canali 1, 6 ed 11 ed impostare gli AP su canali differenti".
- Configurare l' SSID sulle postazioni remote utilizzando lo stesso nome ovvero lo stesso SSID in uso sulla postazione principale.

  (Incredibile!) Utilizzare lo stesso SSID (su una rete "roaming") è veramente molto più semplice. Si può fare l'associazione con un AP una sola volta e il vostro PC o MAC saranno associati con tutti gli AP nella rete WDS senza fare altre operazioni – è veramente molto più facile in questo modo.

  Bisogna però ricordare che non si deve fare questa operazione. Al contrario si deve assegnare a ciascun AP un SSID unico e quindi si deve configurare il proprio computer per associarlo agli AP in base alle proprie necessità.
- Assicurarsi di disattivare qualsiasi funzionalità di routing o DHCP nelle postazioni ripetitori. Tali funzionalità dovrebbero essere effettuate dalla postazione base principale o dal router principale della rete.

Solo WDS (Wireless Distribution System)

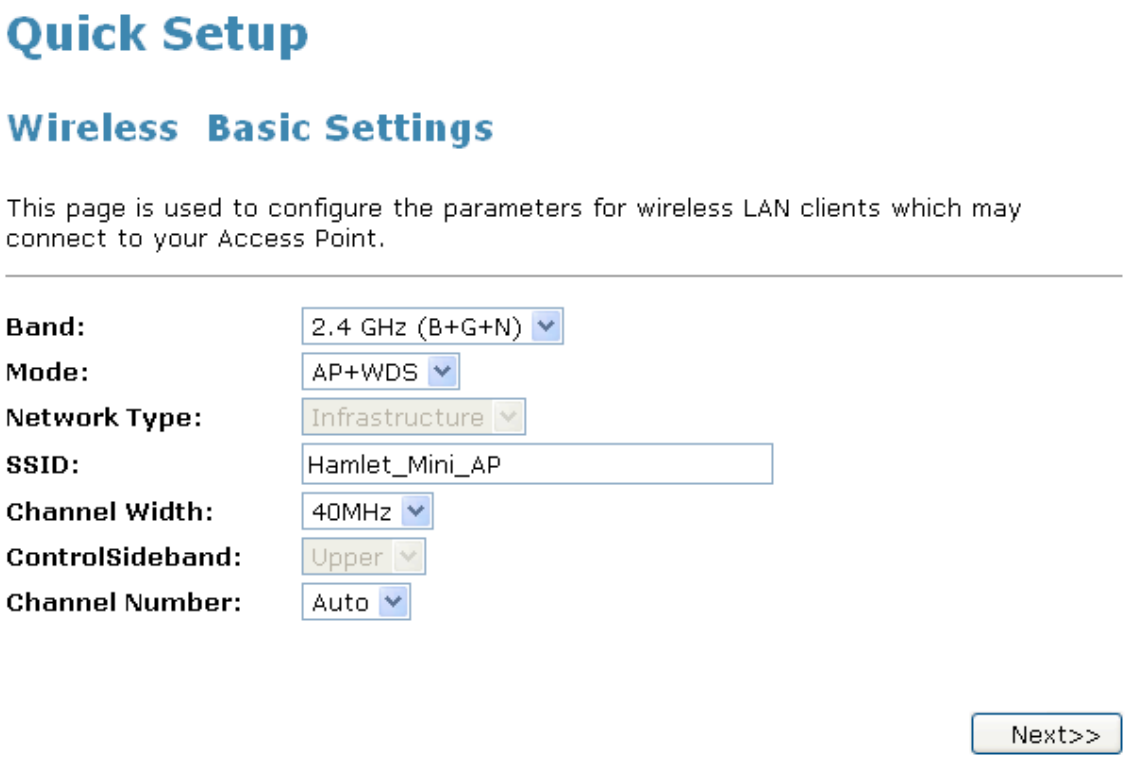
1. Selezionare dall'elenco del campo *Band* un valore di Banda opportuno.
2. Selezionare dall'elenco del campo *Mode* l'opzione *WDS*.
3. Selezionare dall'elenco del campo *Channel Width* un valore opportuno per la larghezza di banda del canale.
4. Selezionare dall'elenco del campo *ControlSideBand* un valore opportuno.
5. Selezionare dall'elenco del campo *Channel Number* il numero da assegnare al canale.
6. Premere il pulsante *Next>>*.



AP (Access Point) + WDS (Wireless Distribution System)

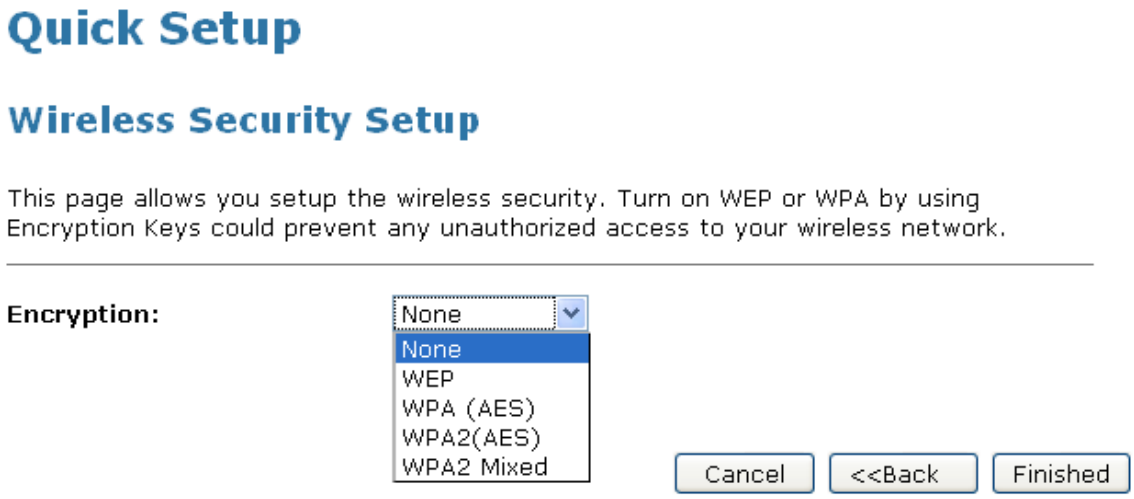
L'Access Point ha la funzione di configurare i parametri dei Client della rete LAN Wireless che si potrebbero collegare all'Access Point stesso.

1. Selezionare dall'elenco del campo *Band* un valore di Banda opportuno.
2. Selezionare dall'elenco del campo *Mode* l'opzione *AP+WDS*.
3. Digitare l' *SSID* (ad esempio 11n Pocket AP).
4. Selezionare dall'elenco del campo *Channel Width* un valore opportuno per la larghezza di banda del canale.
5. Selezionare dall'elenco del campo *ControlSideBand* un valore opportuno.
6. Selezionare dall'elenco del campo *Channel Number* il numero da assegnare al canale.
7. Premere il pulsante *Next>>*.



Configurazione Wireless Security

Questa pagina permette di configurare la sicurezza della connessione wireless. L'attivazione di tecniche quali WEP o WPA che utilizzano chiavi di protezione possono prevenire accessi non autorizzati alla rete wireless.



E' possibile proteggere i dati nella rete wireless da potenziali *intercettatori*, mediante tecniche di cifratura dei dati trasmessi. Un possibile intercettatore potrebbe configurare un adattatore wireless compatibile al vostro adattatore e, posizionandolo opportunamente nel range operativo, realizzare la connessione alla vostra rete. Per difendersi da tale condizione, è possibile applicare la "cifratura" dei dati, che consiste nella traslazione dei dati stessi in una forma difficilmente comprensibile da utenti non autorizzati.

Esistono due tecniche per rendere più sicure le reti wireless:

- *Wired Equivalent Privacy (WEP)*; i dati sono cifrati in blocchi di lunghezza pari a 64 o 128 bit. I dati così cifrati possono quindi essere inviati e ricevuti dai soli utenti che conoscono la chiave di cifratura utilizzata. Ciascun PC connesso alla rete wireless deve essere configurato singolarmente con la stessa chiave del Router allo scopo di cifrare le trasmissioni dei dati sulla rete wireless. Gli intercettatori non possono accedere alla rete senza conoscere la chiave in uso. Il metodo WEP è considerato un sistema con basso livello di protezione.
- *Wi-Fi Protected Access (WPA)*; utilizza un metodo più compleso e sicuro di cifratura dei dati (chiamato TKIP - Temporal Key Integrity Protocol). Tale metodo si avvia in modalità Pre-Shared Key (PSK) (configurazione agevolata per reti residenziali), che consente di digitare una frase di accesso (pass phrase) su tutti i dispositivi connessi alla rete. La tecnica crittografica WPA utilizza una chiave WPA primaria (detta WPA master key). La WPA master key è derivata dalla frase di accesso (pass phrase) e dal nome della rete (SSID) a cui il dispositivo è connesso.

Per configurare la tipologia di sicurezza da applicare alla propria rete Wireless è possibile selezionare una delle seguenti opzioni:

- Nessun livello di sicurezza sulla rete Wireless: nel campo *Encryption* selezionare l'opzione *None* e quindi premere il pulsante *Finished*. *None* è la selezione di default, ma **si consiglia vivamente** di modificare il livello della sicurezza sulla rete wireless, impostando un diverso valore nel campo.
- WEP 64bit ASCII (5 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WEP a 64bit ASCII (5 caratteri)*.
- WEP 64bit Hex (10 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WEP a 64bit Hex (10 caratteri)*.

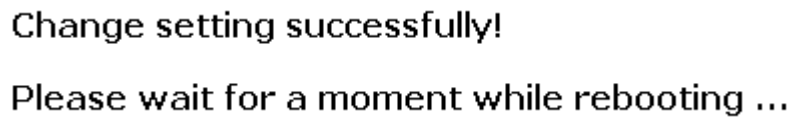
- WEP 128bit ASCII (13 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WEP a 128bit ASCII (13 caratteri)*.
- WEP 128bit Hex (26 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WEP a 128bit Hex (26 caratteri)*.
- WPA (AES) - Wi-Fi Protected Access (AES) Passphrase: seguire le istruzioni del paragrafo *Configurare la tecnica WPA (AES) Passphrase*.
- WPA (AES) - Wi-Fi Protected Access (AES) hex (64 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WPA2 (AES) HEX (64 caratteri)*.
- WPA2 (AES) - Wi-Fi Protected Access 2 (AES) Passphrase: seguire le istruzioni del paragrafo *Configurare la tecnica WPA2 (AES) Passphrase*.
- WPA2 (AES) - Wi-Fi Protected Access 2 (AES) HEX (64 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WPA2 (AES) HEX (64 caratteri)*.
- WPA2 Mixed - Wi-Fi Protected Access 2 (Mixed) Passphrase: seguire le istruzioni del paragrafo *Configurare la tecnica WPA2 (Mixed) Passphrase*.
- WPA2 Mixed - Wi-Fi Protected Access 2 (Mixed) HEX (64 caratteri): seguire le istruzioni del paragrafo *Configurare la tecnica WPA2 (Mixed) HEX (64 caratteri)*.

Configurare la tecnica WEP 64bit ASCII (5 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura a 64 bit.

1. Selezionare nel campo *Encryption* l'opzione *WEP*.
2. Selezionare nel campo *Key Length* l'opzione *64-bit*.
3. Selezionare nel campo *Key Format* l'opzione *ASCII (5 characters)*.
4. Digitare la chiave nel relativo campo *Key Setting*.
5. Premere *Finished*.

6. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.

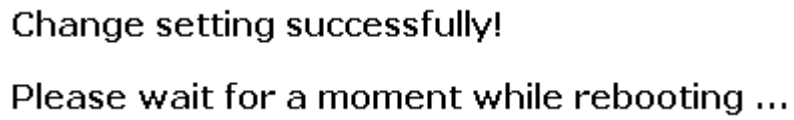


Configurare la tecnica WEP 64bit Hexl (10 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura a 64 bit.

1. Selezionare nel campo *Encryption* l'opzione *WEP*.
2. Selezionare nel campo *Key Length* l'opzione *64-bit*.
3. Selezionare nel campo *Key Format* l'opzione *Hex (10 characters)*.
4. Digitare la chiave nel relativo campo *Key Setting*.
5. Premere *Finished*.

6. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.

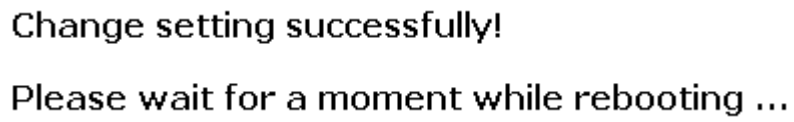


Configurare la tecnica WEP 128bit ASCII (13 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura a 128 bit.

1. Selezionare nel campo *Encryption* l'opzione *WEP*.
2. Selezionare nel campo *Key Length* l'opzione *128-bit*.
3. Selezionare nel campo *Key Format* l'opzione *ASCII (13 characters)*.
4. Digitare la chiave nel relativo campo. *Key Setting*.
5. Premere *Finished*.

6. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.

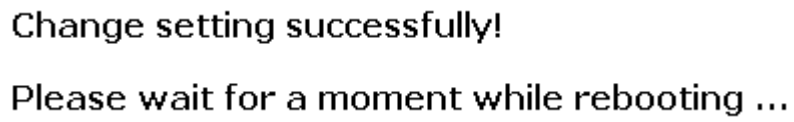


Configurare la tecnica WEP 128bit Hex (26 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura a 128 bit.

1. Selezionare nel campo *Encryption* l'opzione *WEP*.
2. Selezionare nel campo *Key Length* l'opzione *128-bit*.
3. Selezionare nel campo *Key Format* l'opzione *Hex (26 characters)*.
4. Digitare la chiave nel relativo campo *Key Setting*.
5. Premere *Finished*.

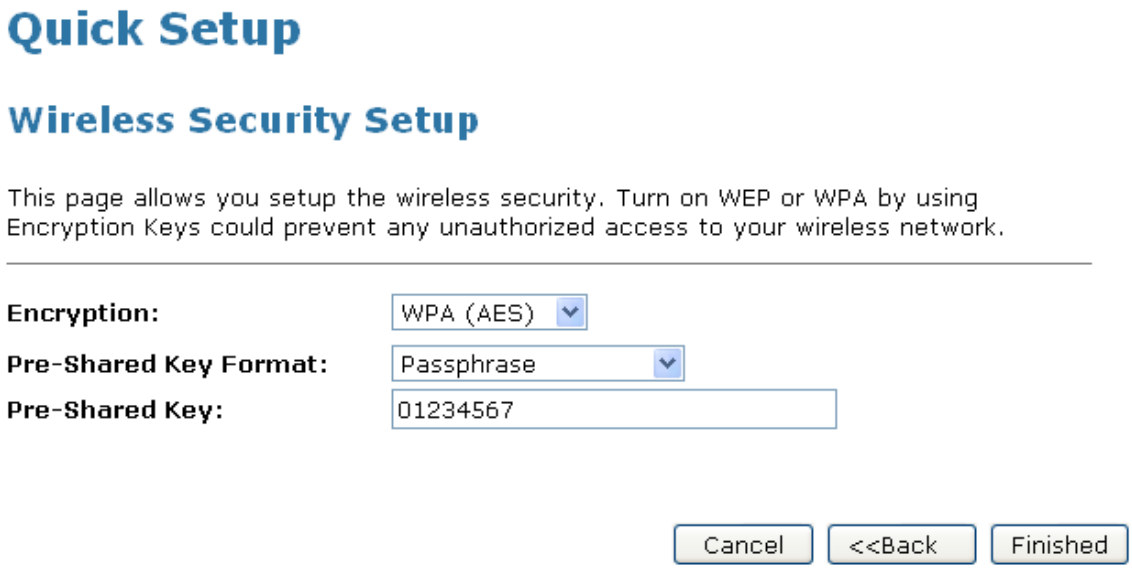
6. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.



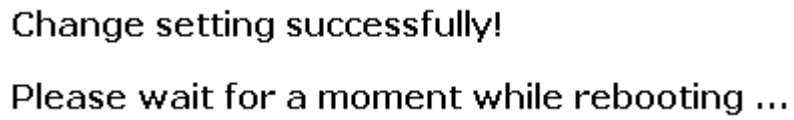
Configurare la tecnica WPA (AES) Passphrase

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura di tipo WPA (AES) Passphrase.

1. Selezionare nel campo *Encryption* l'opzione *WPA (AES)*.
2. Selezionare nel campo *Pre-Shared Key Format* l'opzione Passphrase.
3. Digitare la chiave nel relativo campo.*Pre-Shared Key*.
4. Premere *Finished*.



5. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.

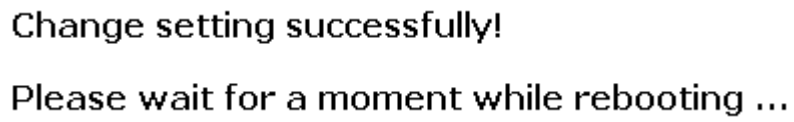


Configurare la tecnica WPA (AES) Hex (64 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura di tipo WPA (AES) HEX (64 caratteri).

1. Selezionare nel campo *Encryption* l'opzione *WPA (AES)*.
2. Selezionare nel campo *Pre-Shared Key Format* l'opzione *HEX (64 characters)*.
3. Digitare la chiave nel relativo campo *Pre-Shared Key*.
4. Premere *Finished*.

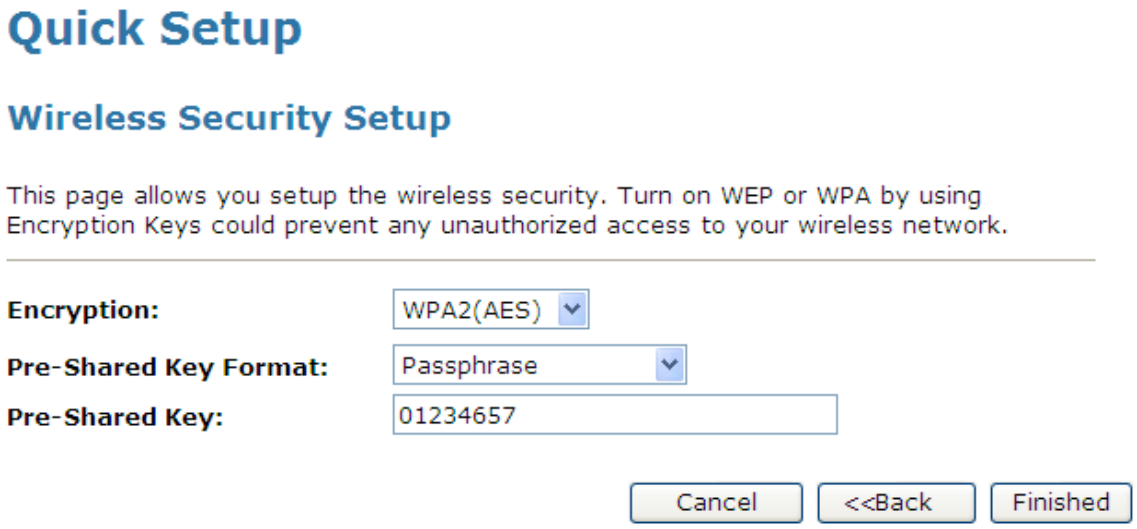
5. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.



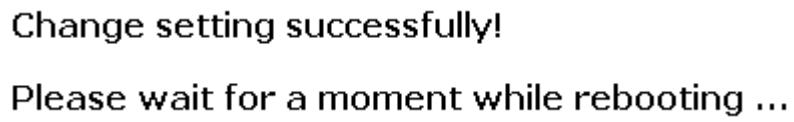
Configurare la tecnica WPA2 (AES) Passphrase

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura di tipo WPA2 (AES) Passphrase.

1. Selezionare nel campo *Encryption* l'opzione *WPA2 (AES)*.
2. Selezionare nel campo *Pre-Shared Key Format* l'opzione *Passphrase*.
3. Digitare la chiave nel relativo campo *Pre-Shared Key*.
4. Premere *Finished*.



5. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.

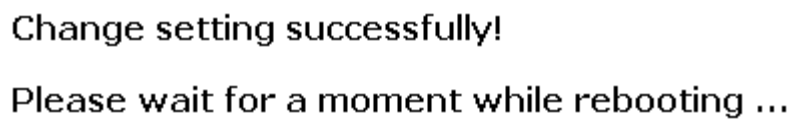


Configurare la tecnica WPA (AES) HEX (64 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura di tipo WPA2 (AES) HEX (64 caratteri).

1. Selezionare nel campo *Encryption* l'opzione *WPA2 (AES)*.
2. Selezionare nel campo *Pre-Shared Key Format* l'opzione *HEX (64 characters)*.
3. Digitare la chiave nel relativo campo *Pre-Shared Key*.
4. Premere *Finished*.

5. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.

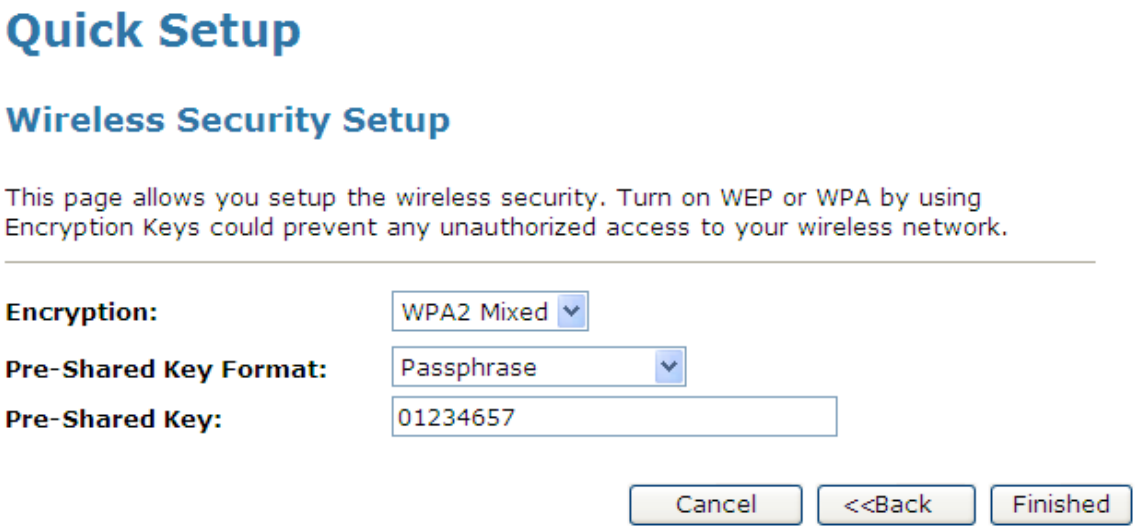


Configurare la tecnica WPA2 (Mixed) Passphrase

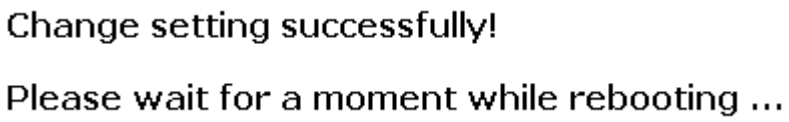
L'esempio riportato di seguito permette di configurare un algoritmo di cifratura di tipo WPA2 (Mixed) Passphrase.

L'algoritmo WPA2 (Mixed) Passphrase supporta entrambi gli algoritmi di cifratura WPA (AES) e WPA2 (AES).

1. Selezionare nel campo *Encryption* l'opzione *WPA2 (Mixed)*.
2. Selezionare nel campo *Pre-Shared Key Format* l'opzione *Passphrase*.
3. Digitare la chiave nel relativo campo *Pre-Shared Key*.
4. Premere *Finished*.



5. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.



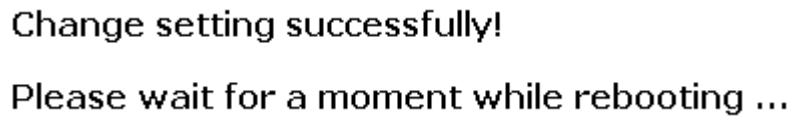
Configurare la tecnica WPA2 (Mixed) HEX (64 caratteri)

L'esempio riportato di seguito permette di configurare un algoritmo di cifratura di tipo WPA2 (Mixed) HEX (64 caratteri).

L'algoritmo WPA2 (Mixed) HEX (64 caratteri) supporta entrambi gli algoritmi di cifratura WPA (AES) e WPA2 (AES).

1. Selezionare nel campo *Encryption* l'opzione *WPA2 (Mixed)*.
2. Selezionare nel campo *Pre-Shared Key Format* l'opzione *HEX (64 characters)*.
3. Digitare la chiave nel relativo campo *Pre-Shared Key*.
4. Premere *Finished*.

5. Si visualizza il messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere mentre si riavvia il dispositivo.



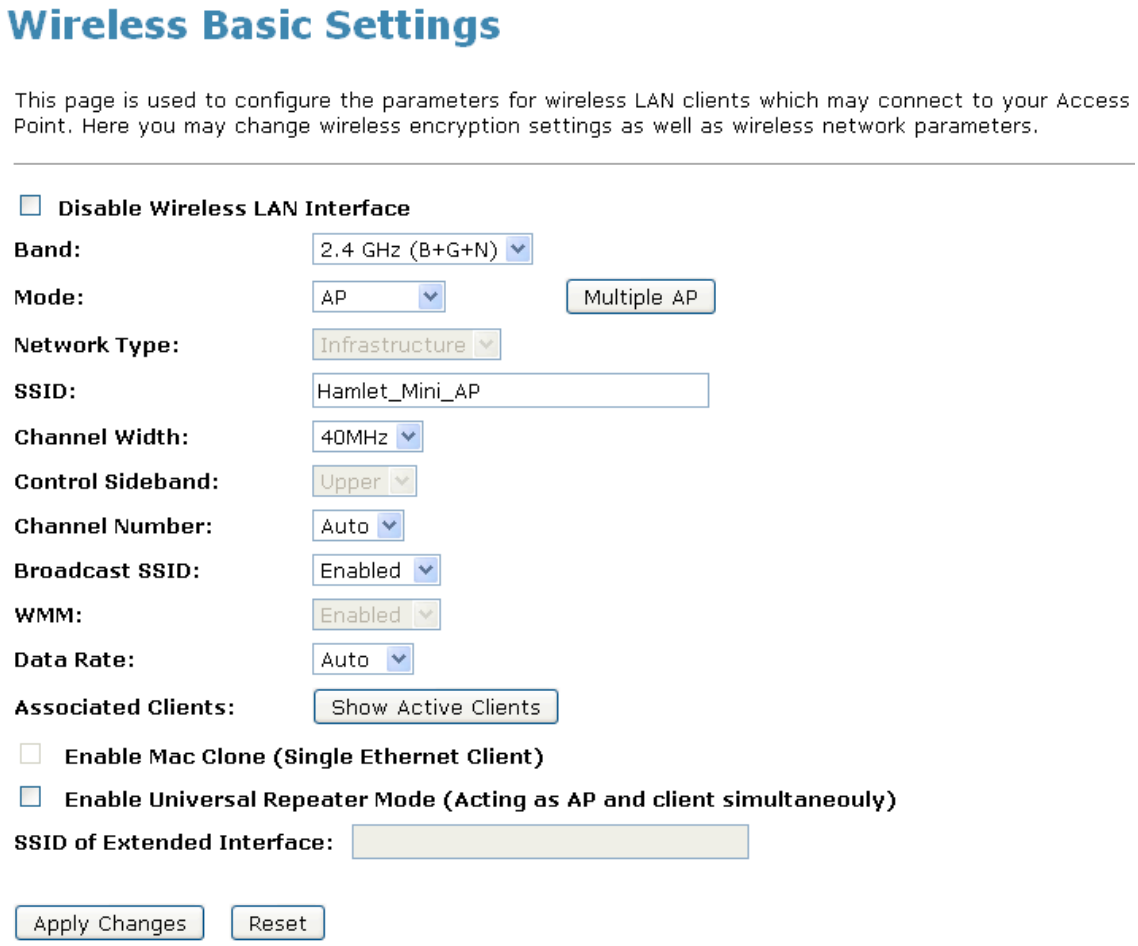
9 Rete Wireless

Il presente capitolo assume che i PC che devono essere collegati siano già correttamente configurati per essere collegati ad una rete wireless e dotati di una scheda di rete idonea. Si veda quanto descritto nella sezione *Configurazione del PC per connessioni alle reti Wireless*.

Configurazioni di base

La pagina *Wireless Network* permette di configurare le caratteristiche basi per la connessione Wireless dell'apparato. Per accedere alla pagina *Wireless Network Basic Settings*:

Dal menù *Wireless* di sinistra selezionare *Basic Settings*. Si visualizza la seguente pagina:



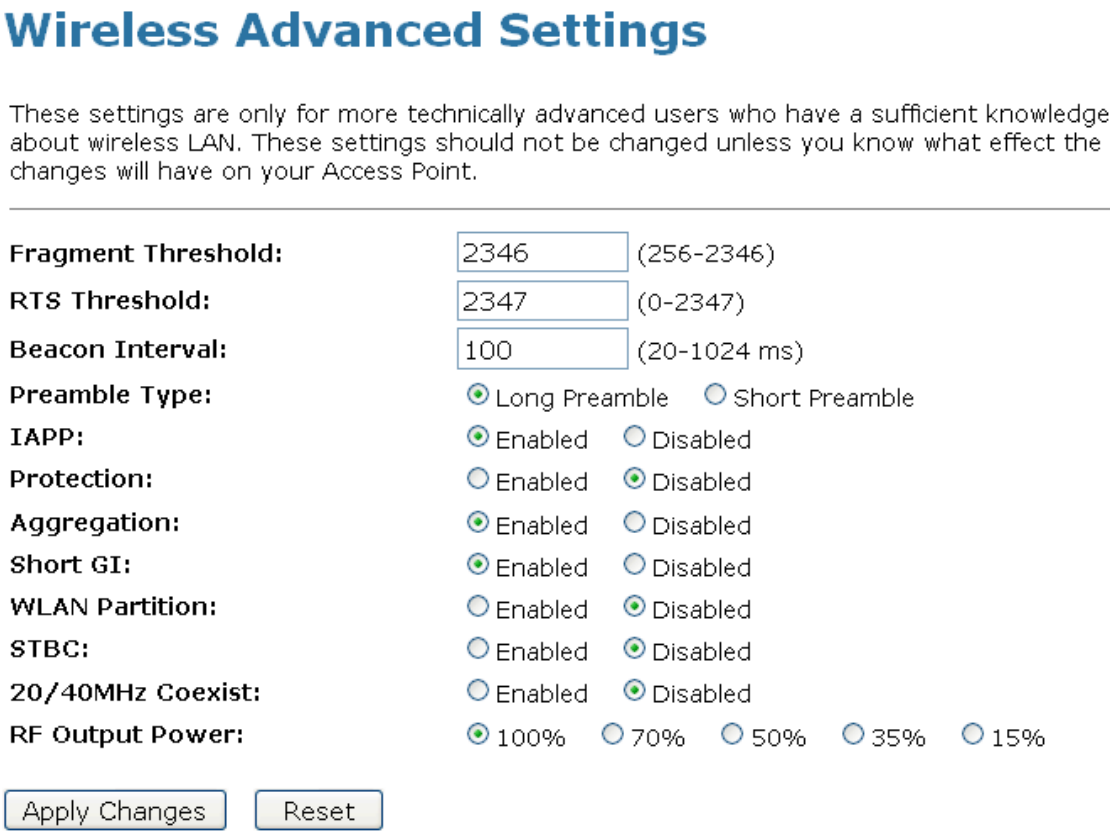
Campo	Descrizione
Disable Wireless LAN Interface	Abilita/disabilita l'interfaccia LAN Wireless. Default: Disabilitata
Band	Specifica la modalità WLAN come 802.11b/g Mixed, 802.11b or 802.11g
Mode	Configura l'interfaccia LAN Wireless in modalità AP, Client, WDS, AP + WDS, MESH o AP + MESH
Network Type	Configura il tipo di rete come Infrastructure o Ad hoc.

SSID	Specifica il nome della rete. Ciascuna rete LAN Wireless uilizza un Nome di Rete unico come identificativo, denominato SSID (Service Set Identifier). In fase di configurazione di un dispositivo wireless, si deve definire il relativo SSID. Per collegarsi ad una rete esistente è necessario specificare il nome di quella rete. Una volta definito il nome della rete, questo deve essere assegnato a tutti i computer della rete. Il nome può avere una lunghezza massima di 20 caratteri e contenere sia lettere che numeri.
Channel Width	Permette di selezionare un Channel Width (larghezza del canale) da un elenco predefinito.
Control Sideband	Permette di selezionare un Control Sideband (controllo della banda laterale) da un elenco predefinito.
Channel Number	Permette di selezionare un Channel Number (numero di canale) da un elenco predefinito.
Broadcast SSID	Definisce l'SSID di rete come Broadcast o SSID nascosta. Default: Enabled (abilitato)
WMM	Abilita/disabilita il suporto Wi-Fi Multimedia (WMM).
Data Rate	Seleziona la velocità di comunicazione (Data Rate) da un elenco predefinito.
Associated Clients	Mostra la tabella Active Wireless Client (tabella dei Client Attivi nella rete Wireless) La tabella mostra per ciascun client della rete Wireless le seguenti informazioni: MAC address, contatore dei pacchetti trasmessi e ricevuti e tipo di protezione.
Enable Mac Clone (Single Ethernet Client)	Abilita l'uso della funzione di duplicazione del Mac (Singola scheda di rete)
Enable Universal Repeater Mode	Opera come AP (Access Point) e Client contemporaneamente
SSID of Extended Interface	Se si imposta la modalità come “AP” e si attiva la funzione URM (Universal Repeater Mode), si dovrebbe inserire l' SSID di un altro AP nel campo “SSID of Extended Interface”. Il numero di canale dovrà essere pari a quello impostato sull'altro AP, poichè dovrà essere condiviso lo stesso canale tra l'AP e l'interfaccia URM (definita in questo caso come interfaccia estesa).

Configurazioni avanzate

Le operazioni di configurazione di seguito descritte sono riservate a soli utenti (esperti) che hanno buona conoscenza delle reti LAN. Tali configurazioni non dovrebbero essere modificate se non se ne conosce l'effetto sull'Access Point. Per accedere alla pagina *Wireless Network Advanced Settings*:

Dal menù *Wireless* di sinistra selezionare *Advanced Settings*. Si visualizza la seguente pagina:


Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
STBC: Enabled Disabled
20/40MHz Coexist: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%
Apply Changes
Reset

Campo	Descrizione
Fragment Threshold	Quando viene trasmesso un pacchetto su un tipo di connessione di rete, può verificarsi la necessità di spezzettare il pacchetto in diversi segmenti, qualora la dimensione dello stesso ecceda la lunghezza massima consentita per quel tipo di connessione. Il campo Fragmentation Threshold (Soglia di frammentazione) definisce il limite per la frammentazione di un messaggio, espresso come numero massimo di byte.
RTS Threshold	RTS è l'acronimo di "Request to Send". Questo parametro controlla la dimensione del pacchetto dati che viene assegnata dal protocollo RF per l'emissione di un pacchetto RTS. Il default è 2347.
Beacon Interval	Seleziona il periodo di riferimento per ottenere il miglior tempo di risposta per i Client Wireles di tipo HTTP.
Preamble Type	Specifica il tipo di Preambolo come "Short" o "Long".
IAPP	Disabilita o abilita la funzione IAPP

Protection	Meccanismo di protezione per prevenire le collisioni dei dati nei nodi di tipo 802.11g.
Aggregation	Disabilita o abilita la funzione Aggregazione dati
Short GI	Disabilita o abilita la funzione Short GI
WLAN Partition	Disabilita o abilita la partizione WLAN
STBC	Disabilita o abilita la funzione STBC
20/40MHz Coexist	Disabilita o abilita la funzione 20/40MHz Coexist
RF Output Power	Misura della potenza in TX.

Sicurezza

Da questa pagina è possibile configurare il livello di sicurezza della propria connessione wireless. L'attivazione di tecniche WEP o WPA con codici (chiavi) di cifratura dei dati, può prevenire accessi non autorizzati alla rete wireless. Per aprire la pagina Wireless Network Security:

Dal menù Wireless di sinistra selezionare Security. Si visualizza la seguente pagina:

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID:
Root AP - Hamlet_Mini_AP
Apply Changes
Reset
Encryption:
Disable
802.1x Authentication:

Campo	Descrizione
Select SSID	Seleziona l' SSID
Encryption	Configura la tecnica di sicurezza (Encryption) come Disable (non attiva), WEP, WPA , WPA2 o WPA-Mixed
Use 802.1x Authentication	Utilizza l'Autenticazione 802.1x per WEP 64bits o WEP 128bits
Authentication	Configura la modalità di autenticazione come Open System (Sistema aperto), Shared Key (chiave condivisa) o Auto
Key Length	Seleziona la lunghezza della chiave di cifratura come 64-bit o 128-bit
Key Format	Seleziona il formato della chiave di cifratura come ASCII (5 caratteri), Hex (10 caratteri), ASCII (13 caratteri) o Hex (26 caratteri)

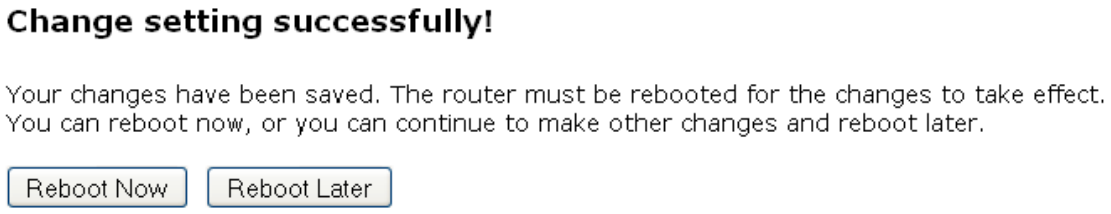
Encryption Key	Campo per l'inserimento della chiave di cifratura
WPA Authentication Mode	Configura la WPA Authentication Mode come Enterprise (RADIUS) o Personal (Pre-Shared Key)
WPA Cipher Suite	Configura la WPA Cipher Suite su AES
Pre-Shared Key Format	Configura la Pre-Shared Key Format come Passphrase o HEX (64 caratteri)
Pre-Shared Key	Campo per l'inserimento della Pre-Shared Key
Enable Pre-Authentication	In conformità alle più diffuse norme, un metodo per stabilire proattivamente un'associazione sicura tra un nodo di tipo 'mobile' ed un agente di autenticazione di una rete (rete in cui il nodo 'mobile' può accedere come visitatore) può essere realizzato utilizzando una flag nell'intestazione di un messaggio. Tale flag ha la funzione di segnalare la richiesta una pre-autenticazione per una connessione sicura. Uno dei due nodi (o il nodo mobile o l'agente di autenticazione) iniziano tale attività inserendo nella header del messaggio la flag di pre-autenticazione; l'atro nodo risponderà con la medesima flag inserita nella header del messaggio, solo se supporta la pre-autenticazione. Il campo Abilita/disabilita il supporto di pre-autenticazione. Default: disabilitato.
Authentication RADIUS Server	Port: numero di porta del Server RADIUS IP address: indirizzo IP del Server RADIUS Password: Password del Server RADIUS

WEP + Encryption Key

La tecnica WEP garantisce la sicurezza della rete mediante cifratura dei dati trasmessi via radio, così da proteggere la comunicazione da un punto ad un altro. Tuttavia, si è visto che la tecnica WEP non è così sicura come si credeva.

1. Selezionare nel campo *Encryption*, l'opzione *WEP*.
2. Selezionare nel campo *Key Length* l'opzione *64-bit* o *128-bit*.
3. Seleziona dall'elenco del campo *Key Format* l'opzione *ASCII (5 characters), Hex (10 characters), ASCII (13 characters)* o *Hex (26 characters)*.
4. Digitare nel campo *Encryption Key* la chave in funzione del formato selezionato: ASCII o esadecimale.
5. Premere il pulsante *Apply Changes*.

6. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

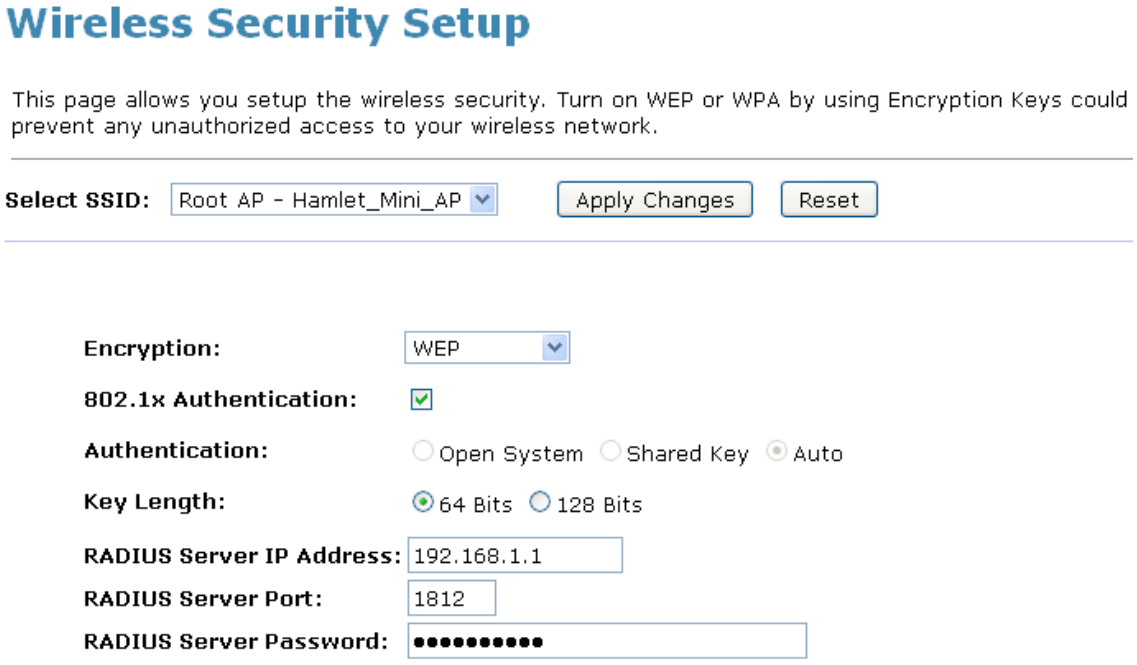

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

WEP + Use 802.1x Authentication

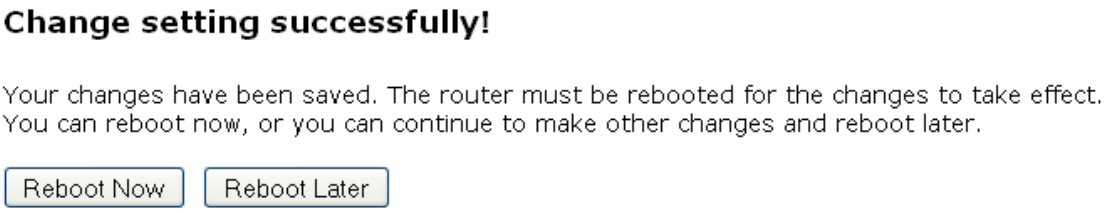
La tecnica WEP garantisce la sicurezza della rete mediante cifratura dei dati trasmessi via radio, così da proteggere la comunicazione da un punto ad un altro. Tuttavia, si è visto che la tecnica WEP non è così sicura come si credeva.

1. Selezionare nel campo *Encryption* l'opzione *WEP*.
2. Selezionare l'opzione *802.1x Authentication*.
3. Selezionare l'opzione *WEP 64bits* o *WEP 128bits*.
4. Digitare il numero di *Porta*, l'*indirizzo IP* e la *Password* del Server RADIUS:

5. Premere il pulsante *Apply Changes*.



6. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

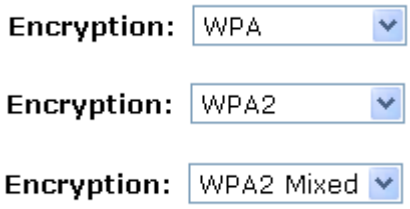

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

WPA/WPA2/WPA2 Mixed + Personal (Pre-Shared Key)

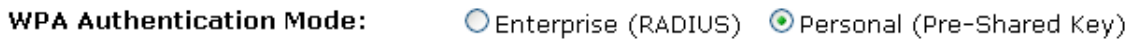
La tecnica Wi-Fi Protected Access (WPA e WPA2) è una classe di sistemi per la sicurezza di reti wireless (Wi-Fi). La WPA è progettata per lavorare con qualsiasi tipo di scheda di rete wireless, ma potrebbe non funzionare con la prima generazione degli Access Point wireless. La tecnica WPA2 implementa lo standard completo, ma non funziona con vecchie schede di rete. Entrambe le tecniche garantiscono un'ottima sicurezza, se si rispettano due condizioni:

- Sia la WPA che la WPA2 devono essere abilitate e preferite rispetto alla tecnica WEP. WEP è normalmente presentata come la prima scelta per la sicurezza in molte istruzioni di installazione.
- In modalità "Personal" (la scelta migliore per reti domestiche e piccoli uffici) si deve impiegare una "frase di accesso" (passphrase) che, per garantire la massima sicurezza, deve essere più lunga di una normale password di 6 - 8 caratteri.

1. Selezionare nel campo *Encryption* l'opzione *WPA*, *WPA2* o *WPA2 Mixed*.



2. Selezionare l'opzione *Personal (Pre-Shared Key)*.

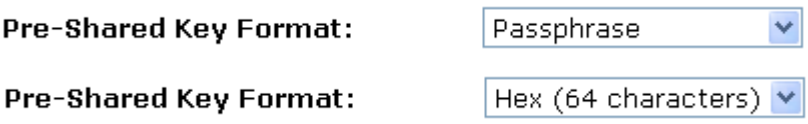


3. Selezionare l'opzione *TKIP* e/o *AES* nella sezione *WPA Cipher Suite*, se il parametro *Encryption* è *WPA*:

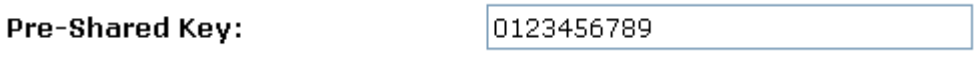
4. Selezionare l'opzione *TKIP* e/o *AES* nella sezione *WPA2 Cipher Suite*, se il parametro *Encryption* è *WPA2*:

5. Selezionare l'opzione *TKIP* e/o *AES* nella sezione *WPA/WPA2 Cipher Suite*, se il parametro *Encryption* è *WPA2 Mixed*:

6. Selezionare nel campo *Pre-Shared Key Format* l'opzione *Passphrase* o *HEX (64 characters)*.

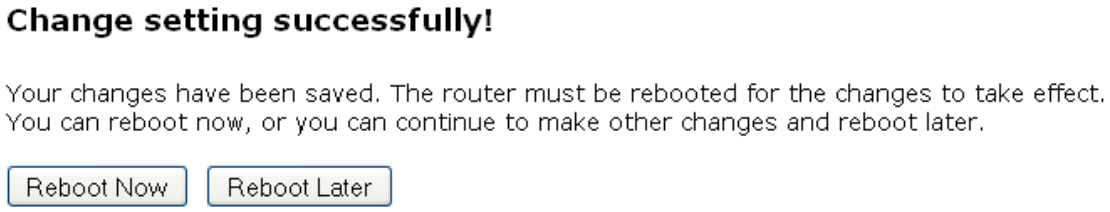


7. Digitare la *Pre-Shared Key* in funzione delal scelta effettuata: *Passphrase* o *Hex (64 caratteri)*.



8. Premere il pulsante *Apply Changes* per confermare e ritornare al menù precedente.

9. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

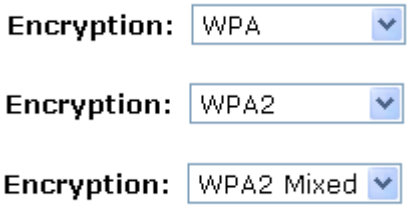

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

WPA/WPA2/WPA2 Mixed + Enterprise (RADIUS)

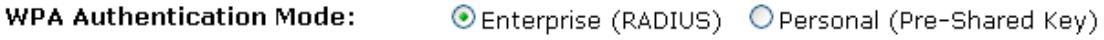
La tecnica Wi-Fi Protected Access (WPA e WPA2) è una classe di sistemi per la sicurezza di reti wireless (Wi-Fi). La WPA è progettata per lavorare con qualsiasi tipo di scheda di rete wireless, ma potrebbe non funzionare con la prima generazione degli Access Point wireless. La tecnica WPA2 implementa lo standard completo, ma non funziona con vecchie schede di rete. Entrambe le tecniche garantiscono un'ottima sicurezza, se si rispettano due condizioni:

- Sia la WPA che la WPA2 devono essere abilitate e preferite rispetto alla tecnica WEP. WEP è normalmente presentata come la prima scelta per la sicurezza in molte istruzioni di installazione.
- In modalità "Personal" (la scelta migliore per reti domestiche e piccoli uffici) si deve impiegare una "frase di accesso" (passphrase) che, per garantire la massima sicurezza, deve essere più lunga di una normale password di 6 - 8 caratteri.

1. Selezionare nel campo *Encryption* l'opzione *WPA*, *WPA2* o *WPA2 Mixed*.



2. Selezionare l'opzione *Enterprise (RADIUS)*.



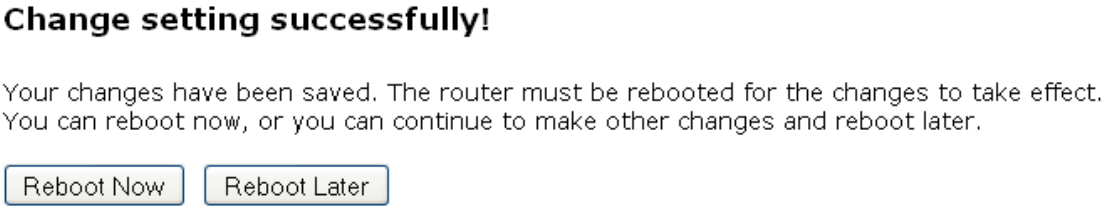
3. Selezionare l'opzione *TKIP* e/o *AES* nella sezione *WPA Cipher Suite*, se il parametro *Encryption* è *WPA*:

4. Selezionare l'opzione *TKIP* e/o *AES* nella sezione *WPA2 Cipher Suite*, se il parametro *Encryption* è *WPA2*:

5. Selezionare l'opzione *TKIP* e/o *AES* nella sezione *WPA/WPA2 Cipher Suite*, se il parametro *Encryption* è *WPA2 Mixed*:

6. Digitare il numero di *Porta*, l'*indirizzo IP* e la *Password* del *Server RADIUS*:

7. Si visualizza il messaggio
Le modifiche sono state correttamente effettuate!
Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

Controllo Accessi

Un ulteriore metodo per incrementare la sicurezza è l'utilizzo di una lista MAC ACL (MAC Address Access List) che risulta essere una ulteriore difficoltà per gli Hacker, nel tentativo di accedere alla rete. E' possibile quindi creare una lista MAC ACL e distribuirla agli AP, così solo le schede di rete autorizzate (il cui MAC address è stato regsitrato) possono connettersi alla rete. Mentre lo spoofing degli indirizzi MAC è un mezzo già collaudato per gli attacchi alla rete degli Hacker, questo può essere utilizzato in combinazione con misure di sicurezza supplementari per aumentare il livello di sicurezza della rete diminuendo di conseguenza la possibilità di una violazione.

Gli indirizzi MAC possono essere aggiunti, cancellati o modificati dalla lista ACL, in funzione dei criteri di accesso.

Se si seleziona 'Allowed Listed', solo i Client il cui indirizzo MAC wireless è presente nella lista si possono collegare tramite l'Access Point. Se si seleziona 'Deny Listed', i Client presenti nella lista non possono collegarsi all'Access Point. Per accedere alla pagina *Wireless Network Access Control*:

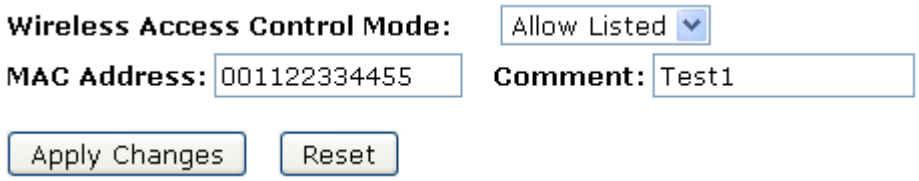
Dal menù *Wireless* di sinistra selezionare Access Control. Si visualizza la seguente pagina:

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Disable
MAC Address:
Comment:
Apply Changes
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

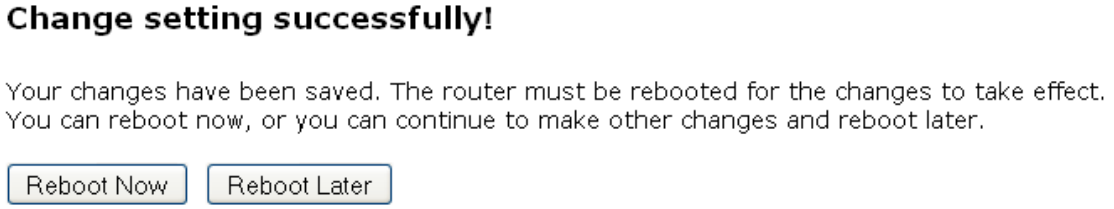
Allow Listed

Se si seleziona 'Allowed Listed', solo i Client il cui indirizzo MAC wireless è presente nella lista si possono collegare tramite l'Access Point.

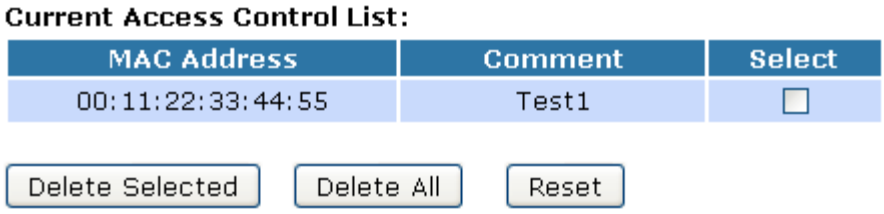
1. Selezionare nel campo *Wireless Access Control Mode*, l'opzione *Allow Listed*.
2. Digitare l'*indirizzo MAC*.
3. Digitare un *commento* esplicativo.
4. Premere il pulsante *Apply Changes*.



5. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

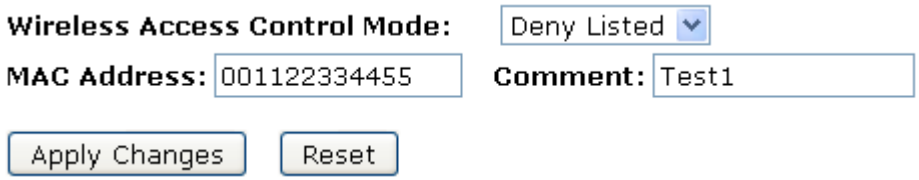
6. L'indirizzo MAC creato viene aggiunto automaticamente alla *Current Access Control List*.



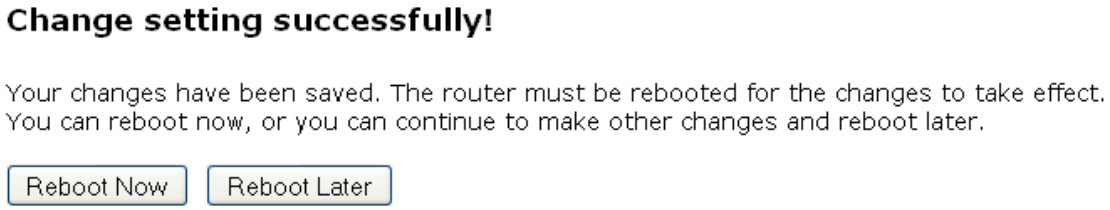
Deny Listed

Se si seleziona 'Deny Listed', i Client presenti nella lista non possono collegarsi all'Access Point.

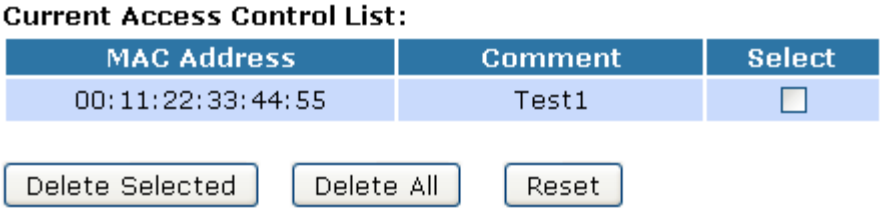
1. Selezionare nel campo *Wireless Access Control Mode*, l'opzione *Deny Listed*.
2. Digitare l'indirizzo MAC.
3. Digitare un *commento* esplicativo.
4. Premere il pulsante *Apply Changes*.



5. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

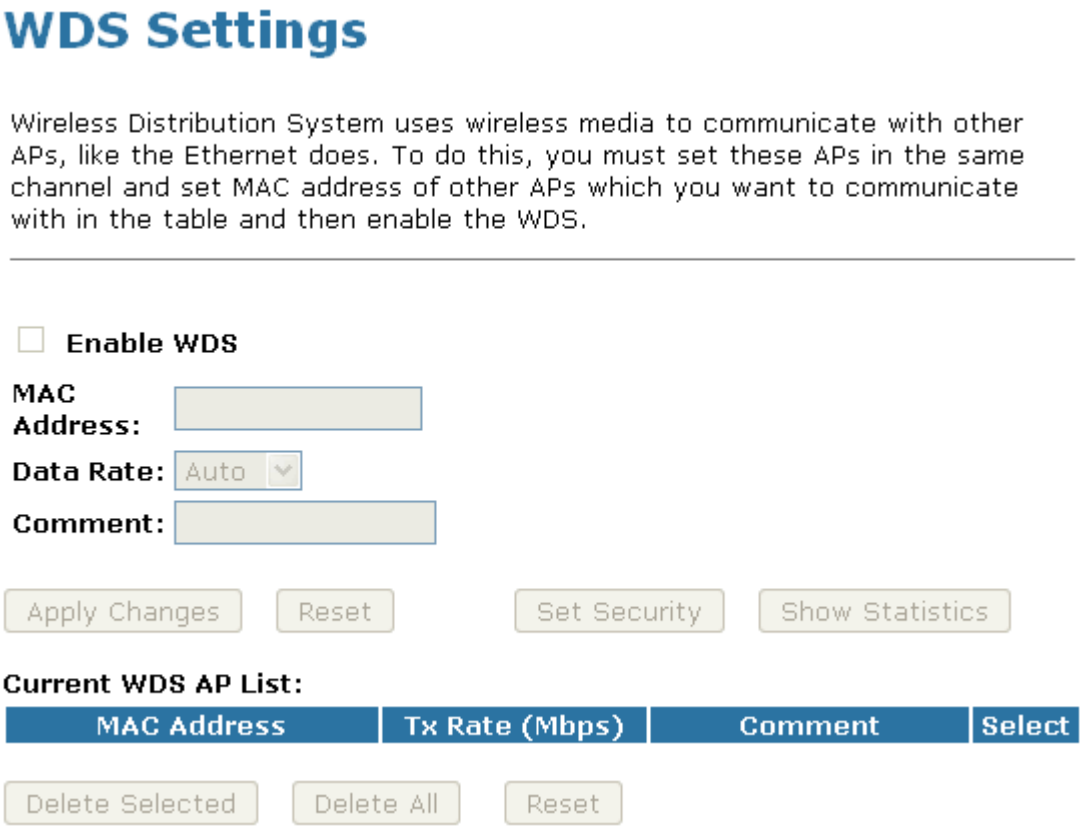
6. L'indirizzo MAC creato viene aggiunto automaticamente alla *Current Access Control List*.



Configurazione WDS

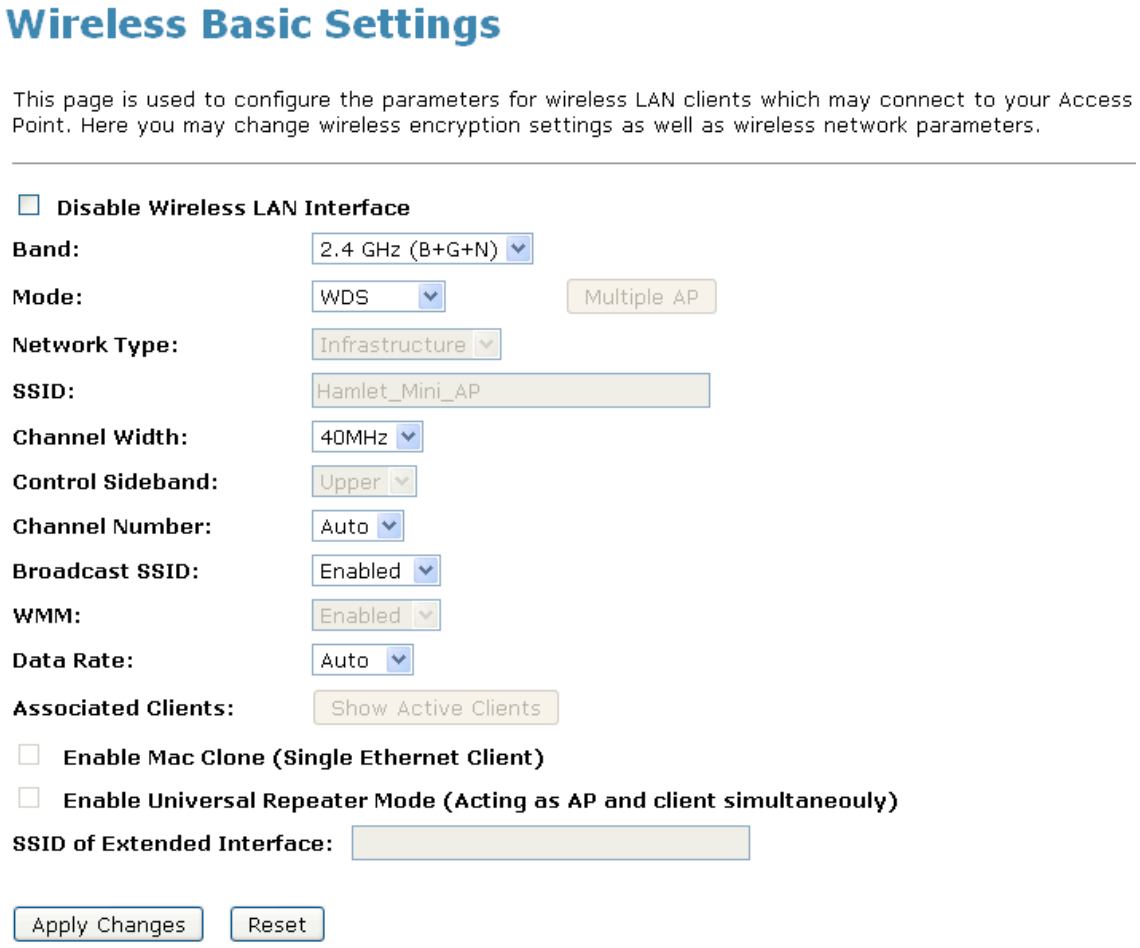
Il sistema Wireless Distribution System utilizza la connessione wireless per comunicare con altri AP, come fosse dispositivi Ethernet. Per attivare tale sistema è necessario predisporre gli AP sullo stesso canale di comunicazione ed impostare nella tabella *Current WDS AP List* l'indirizzo MAC degli AP con cui si vuole comunicare ed infine abilitare la modalità WDS. Per accedere alla pagina *Wireless Network WDS*:

Dal menù *Wireless* di sinistra selezionare *WDS Settings*. Si visualizza la seguente pagina:

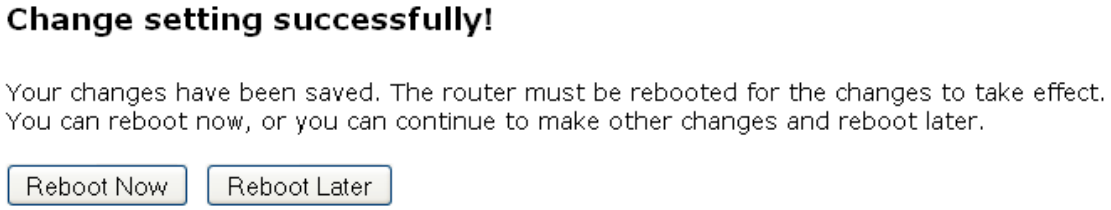

WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
Data Rate:
Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

Configure WDS (Wireless Distribution System) only

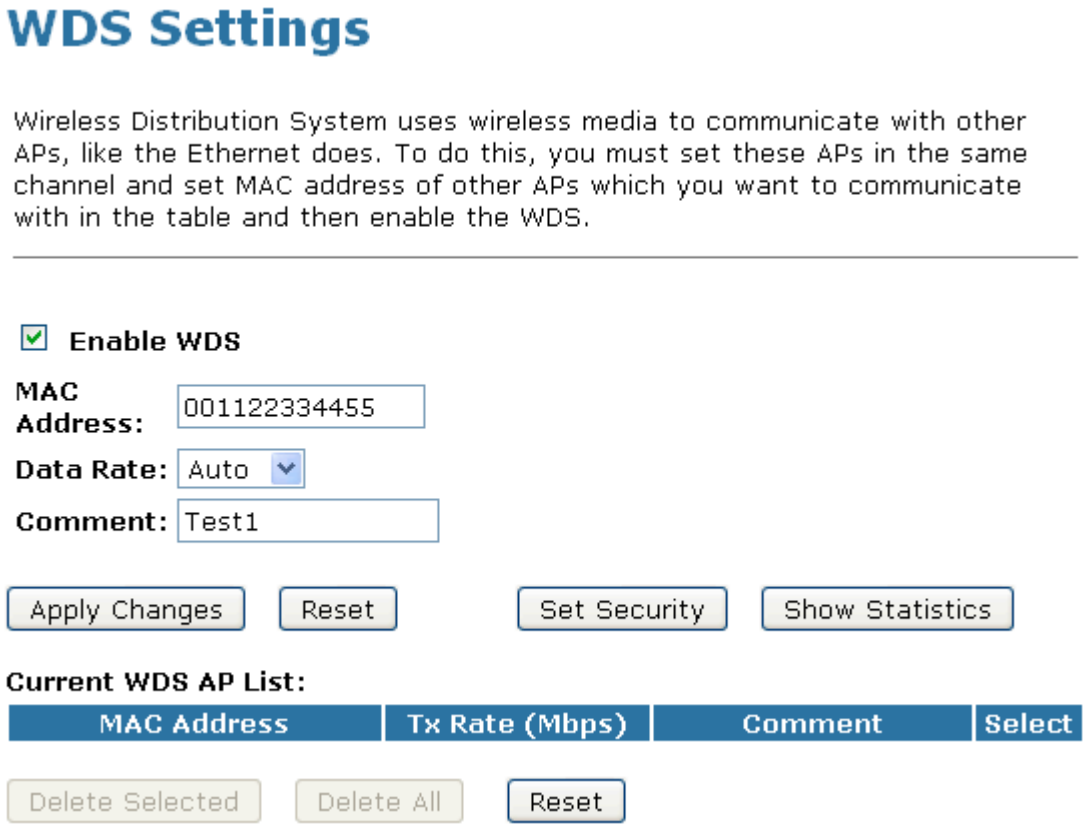
1. Dal menù *Wireless* di sinistra selezionare *Basic Settings*.
2. Selezionare nel campo *Mode* l'opzione *WDS*.
3. Selezionare nel campo *Channel Number* il canale.
4. Premere il pulsante *Apply Changes*.



5. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

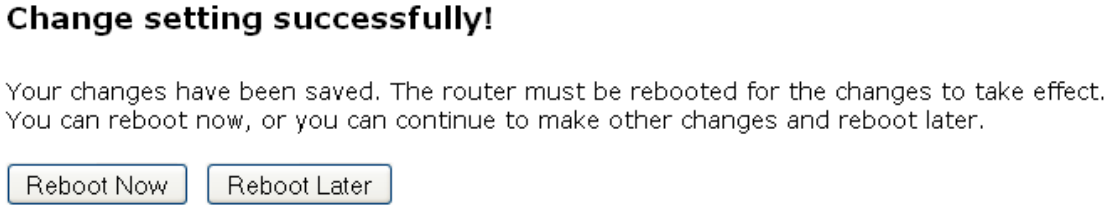

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

6. Dal menù *Wireless* di sinistra selezionare *WDS Settings*.
7. Selezionare l'opzione *Enable WDS*.
8. Digitare l'*indirizzo MAC*.
9. Digitare un *commento* esplicativo.
10. Premere *Set Security*.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
001122334455
Data Rate:
Auto
Comment:
Test1
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

11. Questa pagina permette di configurare la sicurezza per il WDS. Quando abilitato, assicurarsi che l'algoritmo di cifratura e la relativa chiave abbiano gli stessi valori su ciascun apparato.
12. Configurare ciascun campo con i valori dell'algoritmo (campo *Encryption*) selezionato.
13. Premere il pulsante *Apply Changes*.

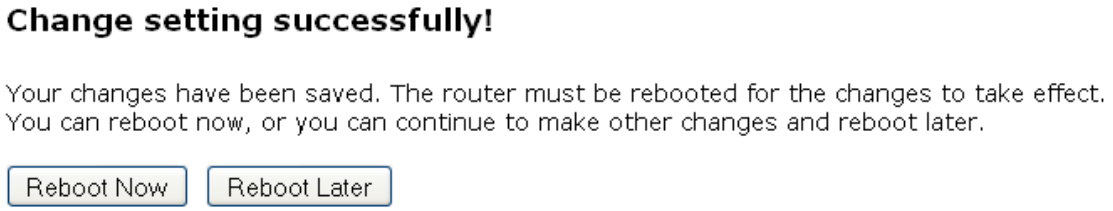
14. Si visualizza il messaggio
Le modifiche sono state correttamente effettuate!
Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

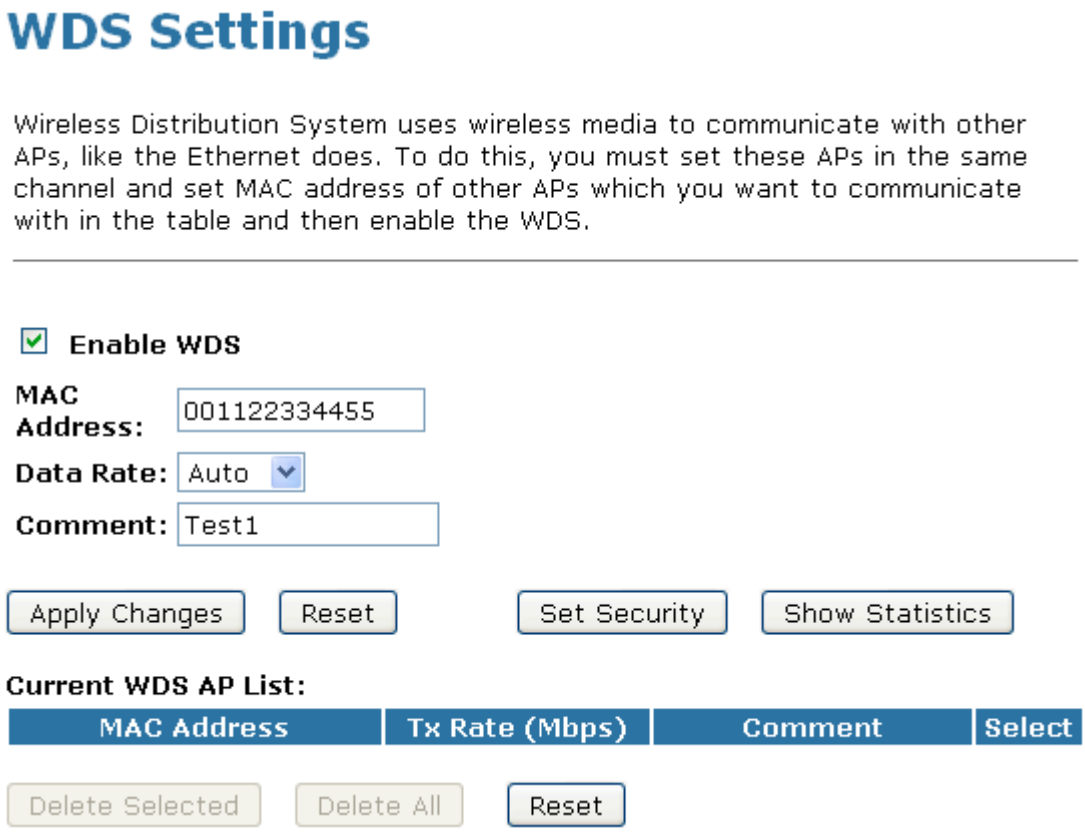
15. Premere il pulsante *Close* per chiudere ed uscire dalla pagina di *WDS Security Setup*.

WDS Security Setup
This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.
Encryption:
None
WEP Key Format:
ASCII (5 characters)
WEP Key:
Pre-Shared Key Format:
Passphrase
Pre-Shared Key:
Apply Changes
Reset

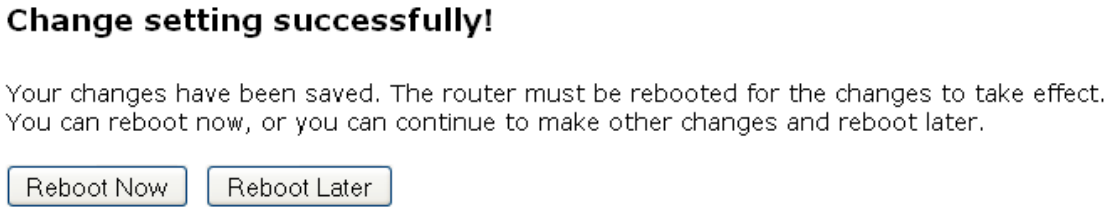
16. Si visualizza il messaggio
Le modifiche sono state correttamente effettuate!
Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

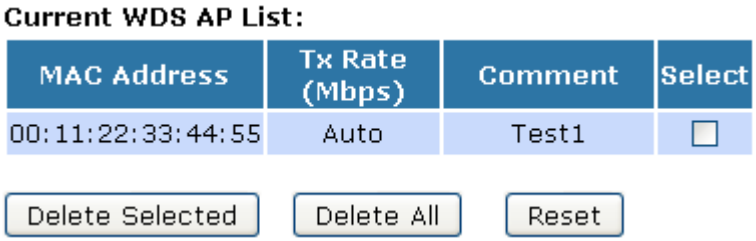
17. Premere il pulsante *Apply Changes*.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
001122334455
Data Rate:
Auto
Comment:
Test1
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

18. Si visualizza il messaggio
Le modifiche sono state correttamente effettuate!
Premere il pulsante *Reboot Now* per confermare.

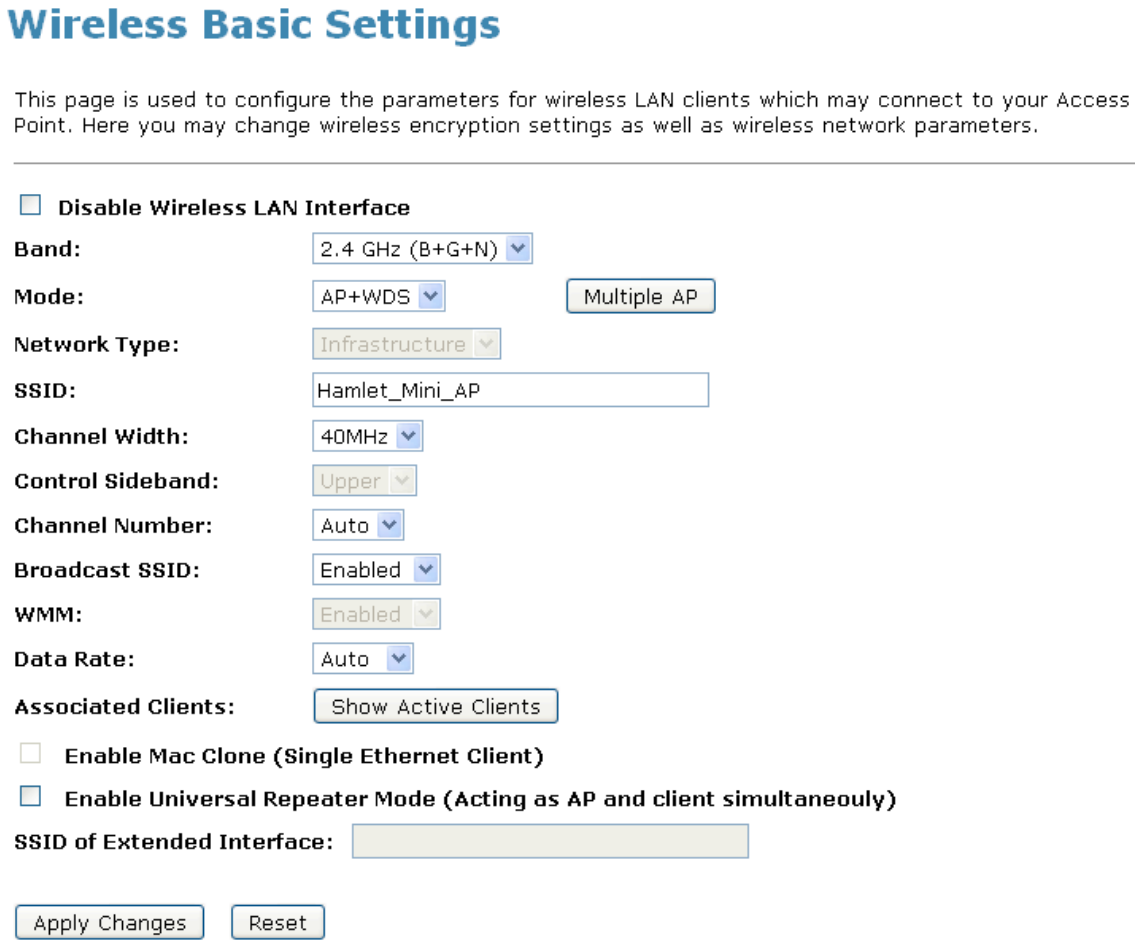

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

19. L'indirizzo MAC creato viene aggiunto automaticamente alla *Current Access Control List*.

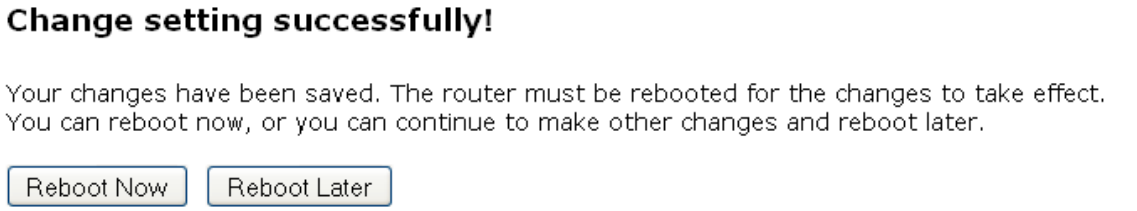


Configurazione AP (Access Point) + WDS (Wireless Distribution System)

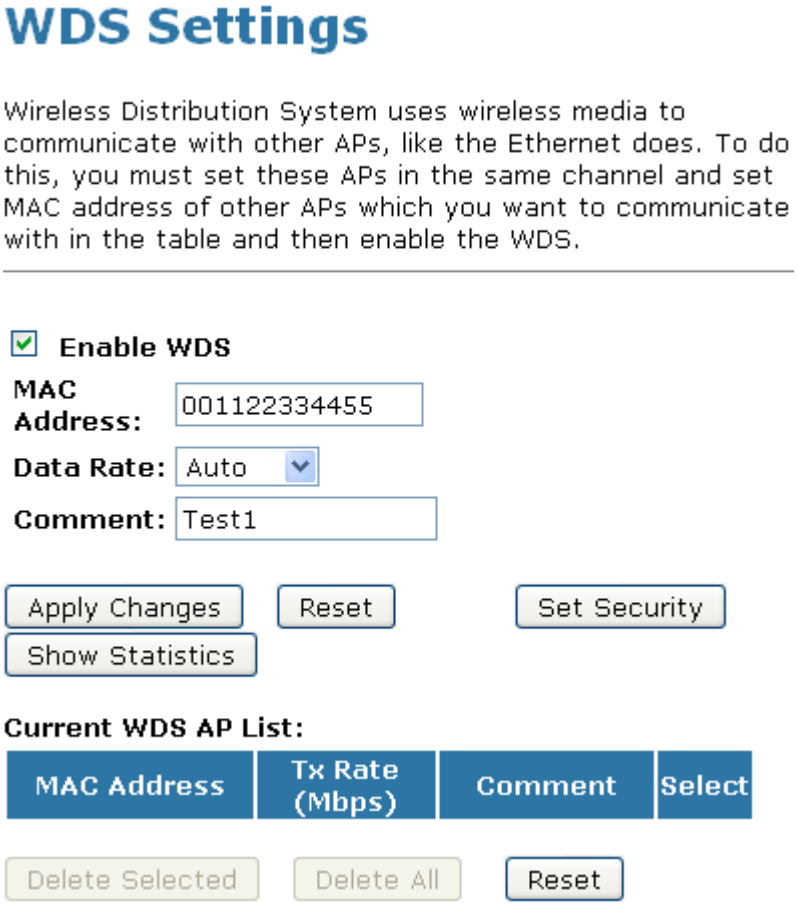
1. Dal menù *Wireless* di sinistra selezionare *Basic Settings*.
2. Selezionare nel campo *Mode* l'opzione *AP+WDS*.
3. Digitare l'*SSID* (ad esempio 11n Pocket AP).
4. Selezionare nel campo *Channel Number* il canale.
5. Premere il pulsante *Apply Changes*.



6. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

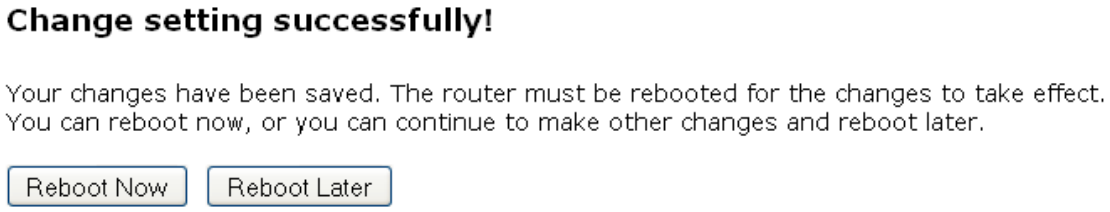

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

7. Dal menù *Wireless* di sinistra selezionare *WDS*.
8. Selezionare l'opzione *Enable WDS*.
9. Digitare l'*indirizzo MAC*.
10. Digitare un *commento* esplicativo.
11. Premere *Set Security*.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
001122334455
Data Rate:
Auto
Comment:
Test1
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

12. Questa pagina permette di configurare la sicurezza per il WDS. Quando abilitato, assicurarsi che l'algoritmo di cifratura e la relativa chiave abbiano gli stessi valori su ciascun apparato.
13. Configurare ciascun campo con i valori dell'algoritmo (campo *Encryption*) selezionato.
14. Premere il pulsante *Apply Changes*.

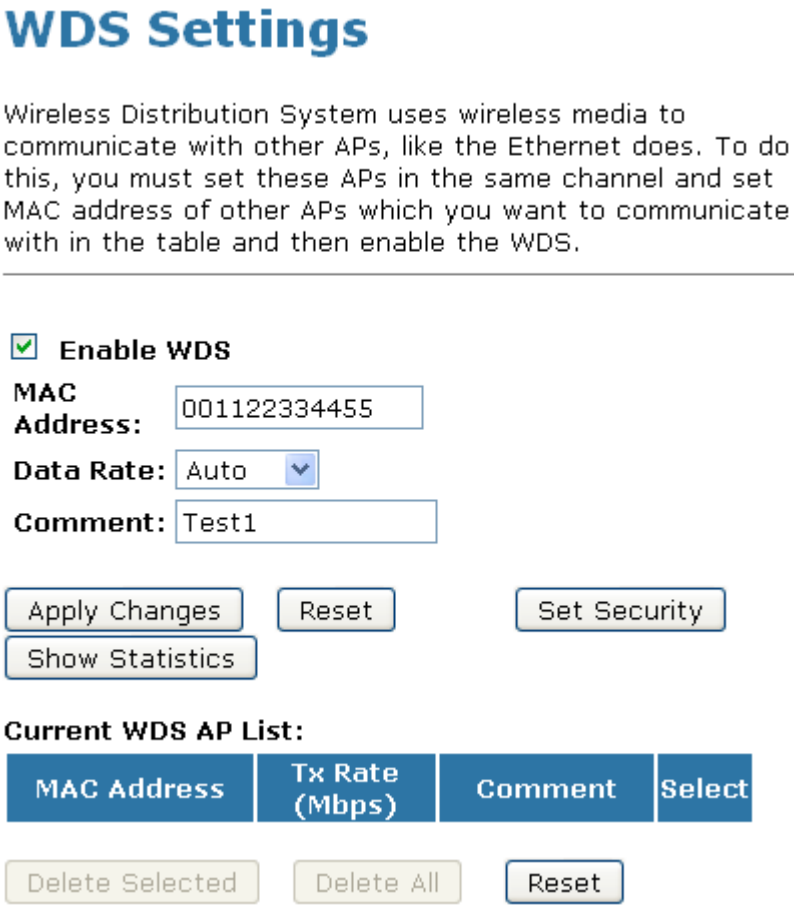
15. Si visualizza il messaggio
    Le modifiche sono state correttamente effettuate!
    Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

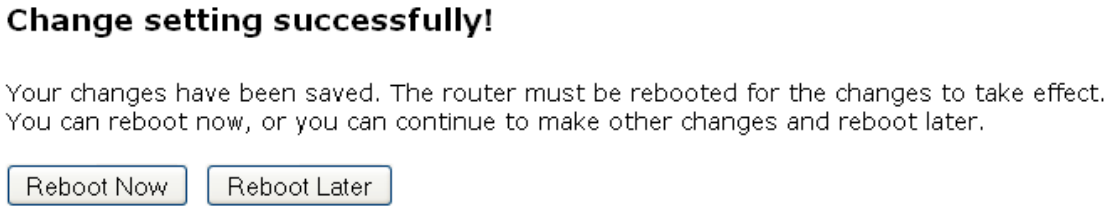
16. Premere il pulsante Close per chiudere ed uscire dalla pagina di *WDS Security Setup*.

WDS Security Setup
This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.
Encryption:
None
WEP Key Format:
ASCII (5 characters)
WEP Key:
Pre-Shared Key Format:
Passphrase
Pre-Shared Key:
Apply Changes
Reset

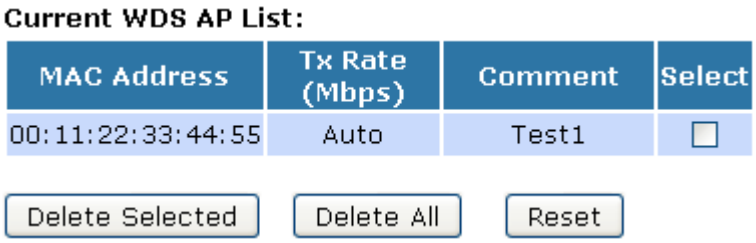
17. Premere il pulsante *Apply Changes*.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
001122334455
Data Rate:
Auto
Comment:
Test1
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

18. Si visualizza il messaggio
Le modifiche sono state correttamente effettuate!
Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

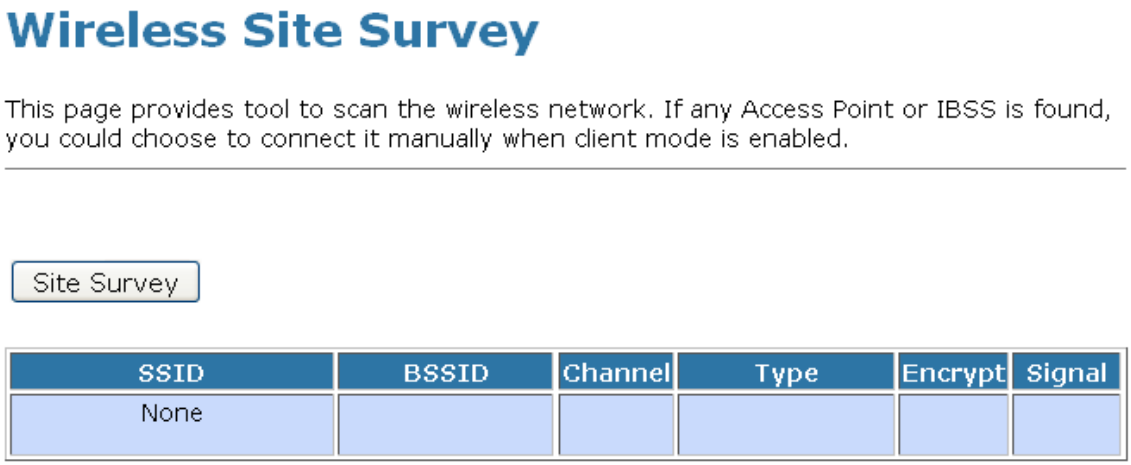
19. L'indirizzo MAC creato viene aggiunto automaticamente alla *Current Access Control List*.



Site Survey (sorveglianza di sito)

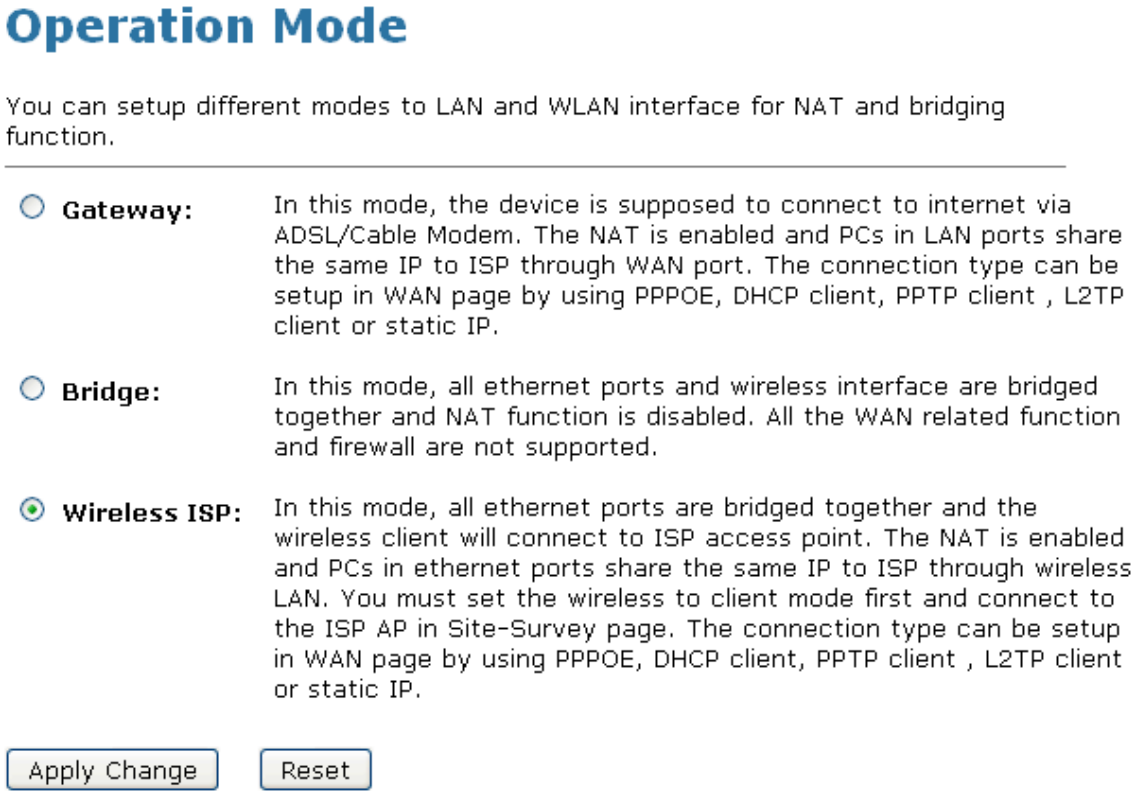
Da questa pagina sono disponibili dei tool per monitorare la rete wireless. Se è presente qualche Access Point o IBSS, si può scegliere di collegarli manualmente quando la modalità Client è abilitata. Per accedere alla pagina *Wireless Network WDS*:

Dal menù *Wireless* di sinistra selezionare *Site Survey*. Si visualizza la seguente pagina:


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Site Survey
SSID
BSSID
Channel
Type
Encrypt
Signal
None

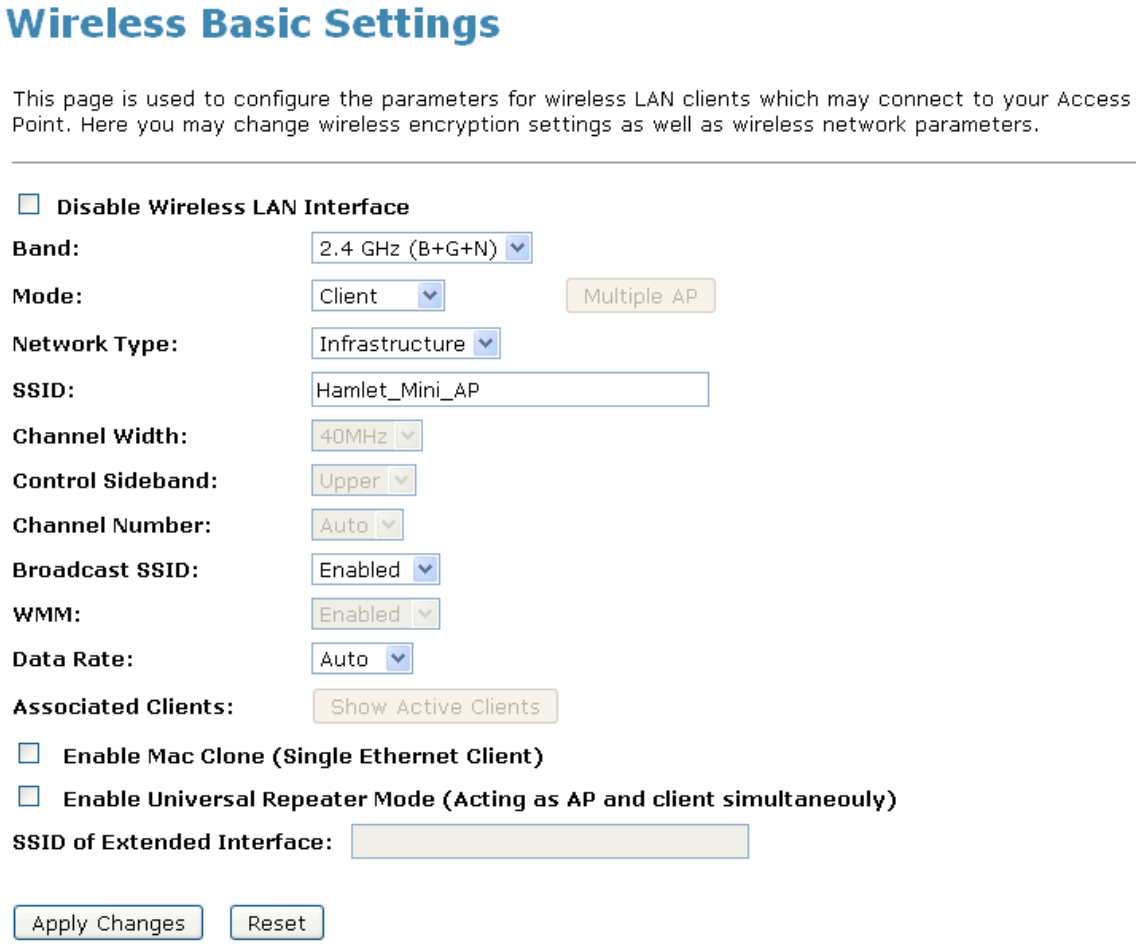
Configurazione Wireless ISP + Wireless client + Site Survey

1. Dal menù *Operation mode* di sinistra selezionare *Wireless ISP Settings*.
2. Premere il pulsante *Apply Changes*.

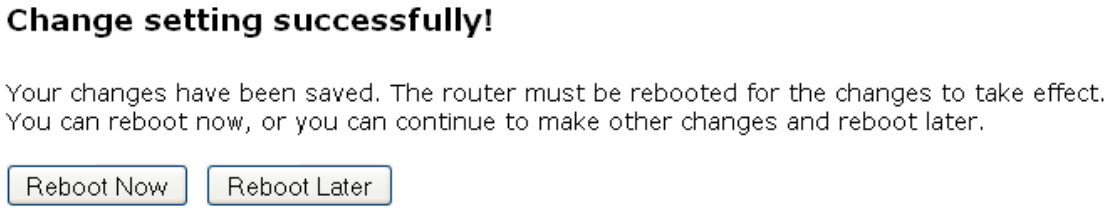

Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Gateway:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
Bridge:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Wireless ISP:
In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
Apply Change
Reset

3. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Non spegnere o riavviare l'apparato.
   Attendere circa 20 secondi ...

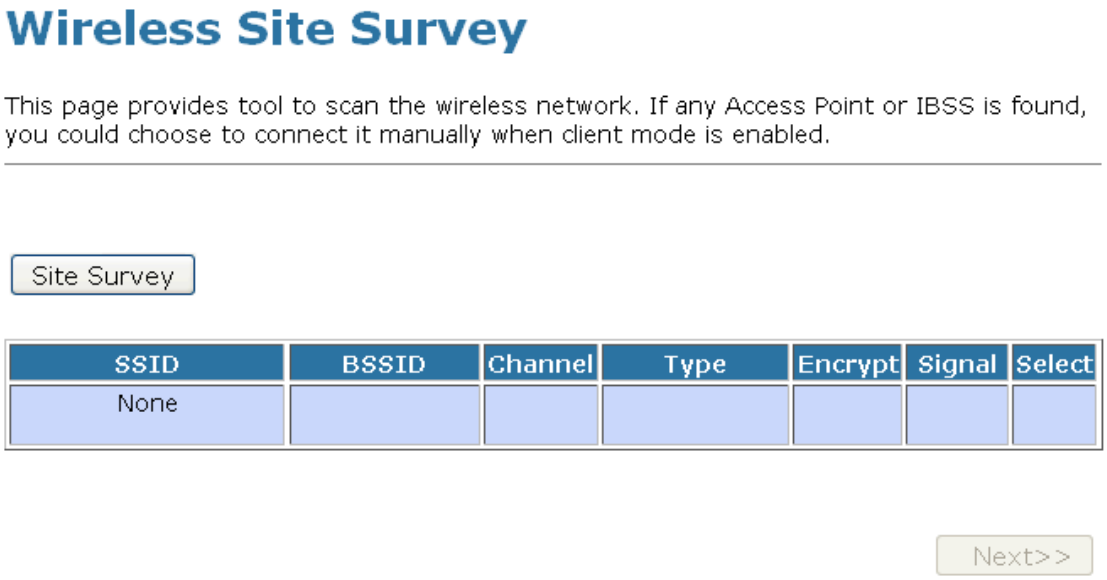
4. Dal menù *Wireless* di sinistra selezionare *Basic Settings*.
5. Selezionare nel campo *Mode* l'opzione *Client*.
6. Digitare l'*SSID* dell'AP che si vuole collegare (ad esempio 11n Pocket AP). Se non si conosce il valore dell'SSID, saltare questa operazione.
7. Premere il pulsante *Apply Changes*.



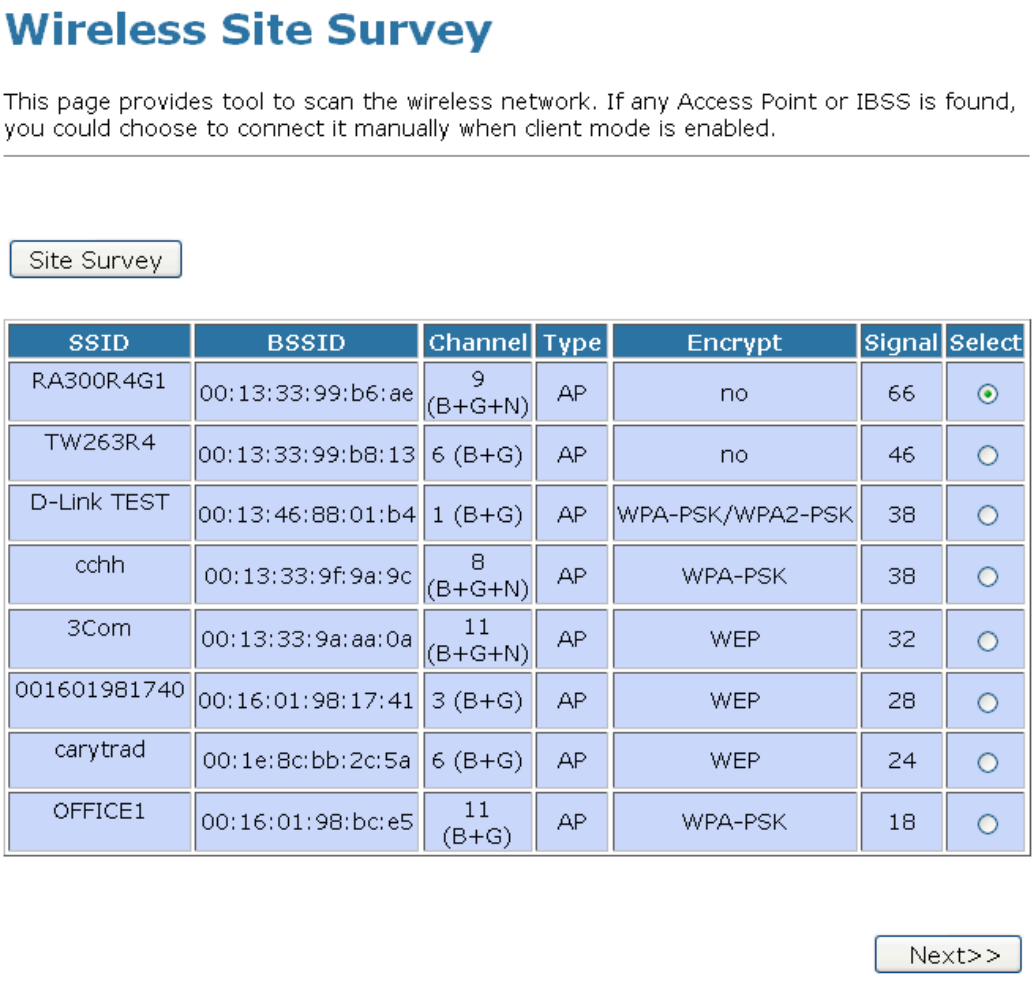
8. Si visualizza il messaggio
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

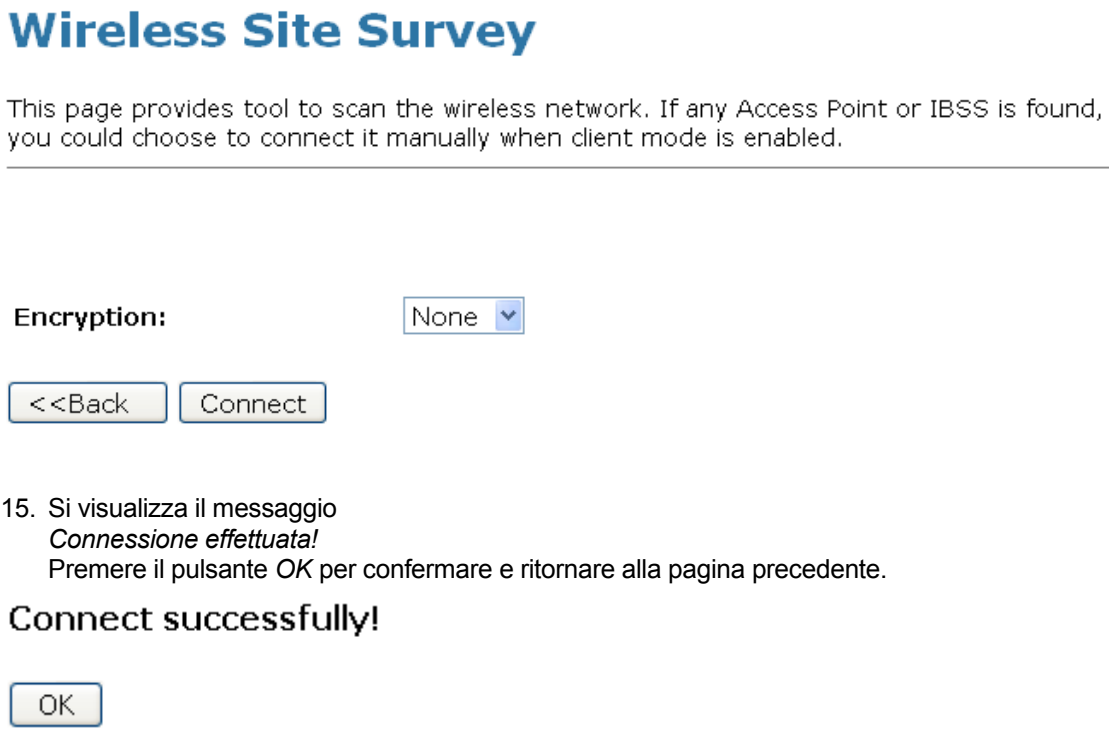
9. Dal menù *Wireless* di sinistra selezionare *Site Survey*.
10. Premere il pulsante *Site Survey*.



11. A questo punto si dovrebbero vedere gli altri AP che sono stati individuati dal Router AP, così come vedere nella tabella sottostante.
12. Dal campo Select, selezionare l'SSID dell'AP che si vuole collegare.
13. Premere il pulsante *Next>>*.



14. Premere nuovamente il pulsante *Next*>>.


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Encryption:
None
<<Back
Connect

15. Si visualizza il messaggio
Connessione effettuata!
Premere il pulsante *OK* per confermare e ritornare alla pagina precedente.

WPS

Questa pagina permette di configurare la funzionalità WPS (Wi-Fi Protected Setup). Tale funzionalità permette di sincronizzare la configurazione di rete sui client associati e collegare in tal modo l' Access Point in un minuto e senza problemi. Per accedere alla pagina *Wireless Network WPS*:

Dal menù *Wireless* di sinistra selezionare *WPS*. Si visualizza la seguente pagina:

Wi-Fi Protected Setup
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.
Disable WPS
WPS Status:
Configured
UnConfigured
Reset to UnConfigured
Self-PIN Number:
62828475
Push Button Configuration:
Start PBC
Apply Changes
Reset
Client PIN Number:
Start PIN

Campo	Descrizione
Disable WPS	Selezionando tale opzione e premendo “Apply Changes” verrà disabilitata la funzione Wi-Fi Protected Setup. Tale funzione è attiva di default.
WPS Status	Quando la configurazione dell'AP è ancora quella di fabbrica, l’apparato è predisposto per sicurezza non attiva ed in stato “un-configured” (non-configurato). Tale messaggio è visualizzato da “WPS Status”. Se si dovesse visualizzare l’indicazione “Configured”, si potrebbe verificare che alcuni “registrars" (quale Vista WCN) non permettano la configurazione dell'AP. In questo caso, sarà quindi necessario accedere alla pagina “Save/Reload Settings” e premere “Reset” per rileggere la configurazione di fabbrica (default).
Self-PIN Number	Il “Self-PIN Number” è il PIN dell'AP. Qualora lo si volesse modificare, sarà necessario premere “Regenerate PIN” e quindi “Apply Changes”. Ulteriormente, se si volesse creare un proprio PIN, sarà necessario digitare quattro cifre senza checksum e quindi premere “Apply Changes”. Tuttavia, tale operazione potrebbe non essere consigliabile finché dal lato registrar sia necessario avere un PIN a quattro cifre.

Campo	Descrizione
Push Button Configuration	Premendo il pulsante *Start PCB* si invoca il metodo PCB del WPS. Si utilizza solamente quando l'AP opera come un Registrar.
Apply Changes	Tutte le volte che si deve abilitare/disabilitare il WPS o cambiare il PIN dell'AP, è necessario premere questo pulsante per attivare le modifiche.
Reset	Ripristina i valori di default del “Self-PIN Number” e del “Client PIN Number”.
Client PIN Number	Si utilizza solo per unire il propriao Router ad una rete di AP (Access Point). La lunghezza del PIN è limitata a quattro o otto cifre numeriche. Se si inseriscono otto caratteri nel PIN con il "checksum error", verrà visualizzato un messaggio di avvertimento. Se si insiste, premendo nuovamente il pulsante, con lo stesso PIN, l'AP lo accetterà automaticamente.

Introduzione al sistema WPS

Da quando le reti wireless domestiche hanno iniziato a diffondersi,diventando sempre più popolari, gli utenti hanno iniziato ad avere problemi nella configurazione della rete. Questo ha fatto sì che gli utenti utilizzassero la rete come rete aperta (senza alcuna tecnica di sicurezza), aumentando il rischio di intercettazioni. Queste sono le motivazioni per cui si progettato il sistema WPS, ossia quello di facilitare la configurazione di reti Wi-Fi e di conseguenza la relativa gesione (Wi-Fi Protected Setup Specification 1.0h.pdf, p.8).

La grossa differenza tra dispositivi con il nuovo sistema WPS ed i precedenti dispositivi è proprio che l'utente, senza avere conoscenze di SSID, canale e sicurezza, può comunque navigare in una rete Wi-Fi con la sicurezza attiva. Ad esempio, in fase di configurazione iniziale della rete, se l'utente vuole configurare il PIN, l'unica cosa che deve fare è quella di digitare il PIN nel registrar, avviare il metodo PIN e quindi attendere finchè il dispositivo si collega alla rete. Dopo aver avviato il metodo PIN da entrambi i lati, un protocollo di registrazione verrà inizializzato tra il registrar e l'enrolle (utente registrato). Tipicamente, un registrar potrebbe essere un access point o un altro dispositivo capace di gestire la rete. Un enrolle potrebbe essere un access point o una postazione che si deve unire alla rete. Dopo lo scambio del protocollo di registrazione, l'enrolle riceverà l'SSID e la configurazione della sicurezza dal registrar, per poi integrarsi nella rete. In altre parole, se una postazione cerca di integrarsi in una rete gestita da un access point con funzioni di registrar, gli utenti dovranno inserire i PIN delle stazioni nella pagina web dell'access point. Se il PIN del dispositivo è corretto e valido e viene avviato di conseguenza anche sulla postazione da collegare, l'access point e la postazione scambieranno automaticamente le informazioni per la tecnica di cifratura della rete, sotto il controllo del registrar interno all'AP. La postazione utilizzerà queste informazioni per eseguire gli algoritmi di autenticazione, integrarsi nella rete sicura e eseguire gli algoritmi di cifratura dei dati durante la trasmissione. Per ulteriori dettagli far riferimento alle successive descrizioni.

Caratteristiche WPS supportate

Attualmente, il Router AP supporta le funzionalità WPS per la modalità **AP**, la modalità **AP+WDS**, la modalità **Infrastructure-Client** e per la modalità ***wireless root interface of Universal Repeater mode***.

Altre modalità, quali la modalità **WDS**, la modalità **Infrastructure-Adhoc** e la modalità ***wireless virtual interface of Universal Repeater mode*** non sono ancora implementate.

Se si forzano le modalità non supportate, il WPS si disabilita automaticamente. Nella configurazione di tutte le modalità WPS supportate, il Router AP ha un *metodo Push Button* ed un *metodo PIN*. Per ciascun metodo, il Router offre differenti livelli di sicurezza per l'accesso in rete, quali ‘Sicurezza aperta’, WEP 64 bits, WEP 128 bits, WPA-Personal TKIP, WPA-Personal AES, WPA2-Personal TKIP e WPA2-Personal AES. L'utente dovrà selezionare il livello ritenuto più idoneo alle proprie esigenze.

Modalità AP

In modalità AP, il Router supporta tre differenti ruoli: registrar, proxy ed enrollee del protocollo di registrazione. In differenti scenari, il Router può commutare automaticamente il proprio ruolo, in funzione del ruolo degli altri dispositivi o per specifiche configurazioni.

AP come Enrollee

Se si conosce il PIN dell'AP e lo si digita nel registrar esterno, il registrar esterno configurerà l'AP con un nuovo profilo di rete quale ad esempio un nuovo SSID ed un nuovo livello di sicurezza. Il registrar esterno efffettua tale operazione sia utilizzando la EAP in banda (wireless) o la UPnP fuori banda (Ethernet). Durante lo scambio messaggi WPS, un profilo Wireless verrà cifrato ed inviato all'AP. Se lo scambio messaggi si realizza correttamente, l' AP sarà reinizializzato con il nuovo profilo wireless e resterà in attesa di collegarsi in rete con postazioni WPS o postazioni precedenti al WPS per unirle alla propria rete.

AP come Registrar

Il Router AP possiede un proprio registrar interno. Se l'utente digita il PIN della postazione nella pagina Web dell' AP e seleziona "Start PBC" ovvero preme il pulsante fisico dell'apparato, l' AP si commuta come registrar automaticamente. Se l'utente effettua la stessa operazione dal lato della postazione da configurare e se lo scambio messaggi WPS avviene correttamente, la configurazione dell'SSID e del livello di sicurezza sarà trasmessa alla postazione senza il rischio di intercettazioni. Quest'ultima si assocerà all'AP in modalità di rete sicura.

AP come Proxy

In questa modalita, l' AP è "trasparente" per gli utenti. Se si vuole configurare una postazione o un qualsiasi dispositivo capace di operare come enrollee, deve digitare il PIN del dispositivo nel registrar esterno e selezionare il profilo wireless corretto. Dopo aver digitato il PIN, il registrar esterno comunicherà tale condizione all'AP. L'AP provvederà quindi a trasferire il profilo criptato dal registrar al dispositivo. Al termine, il dispositivo potrà utilizzare il profilo wireless ed associarsi all'AP. Si tenga però presente che il dispositivo potrebbe connettersi ad altri Access Point se il profilo wireless non appartiene anche al proxy AP. Si dovrà quindi prestare la massima attenzione nel selezionare o creare il profilo utente sul registrar esterno.

Modalità Infrastructure-Client

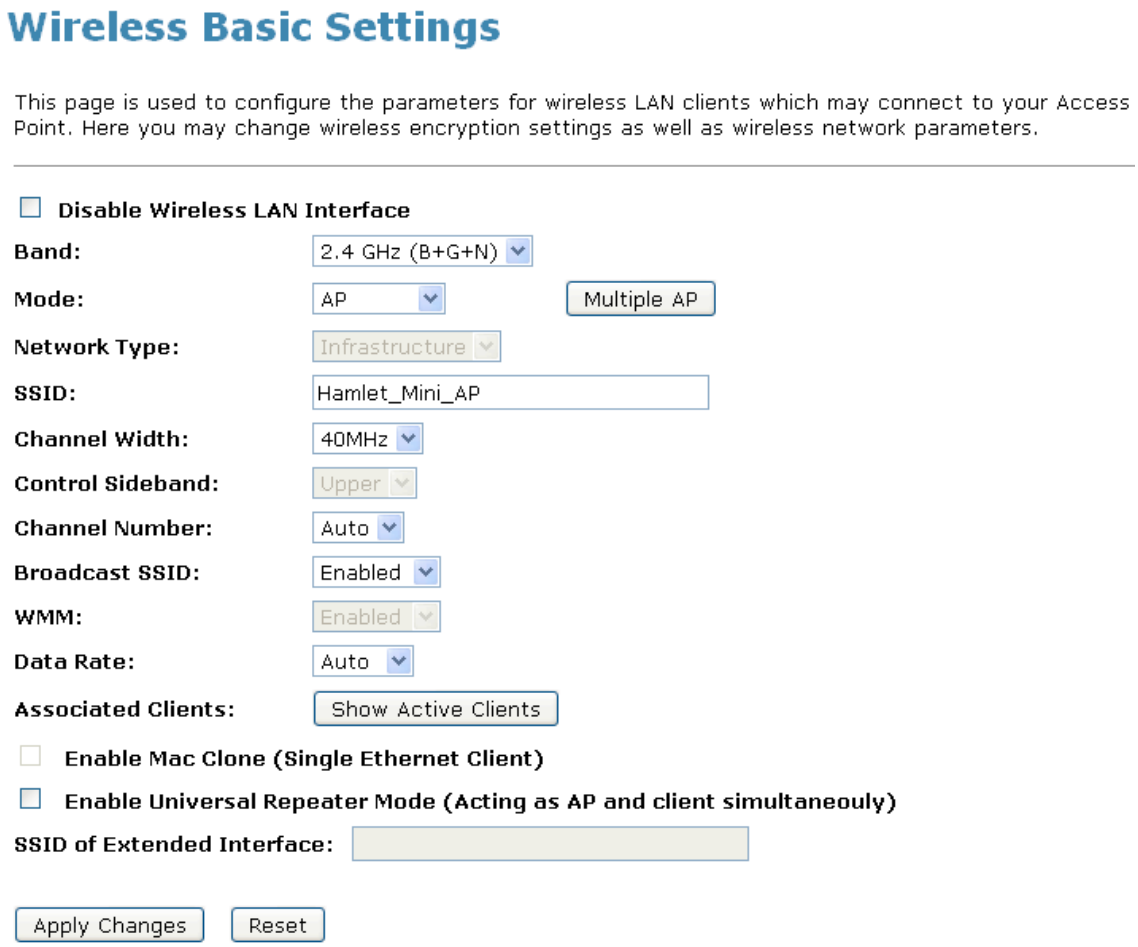
Nella modalità Infrastructure-Client, il Router supporta solamente il ruolo di enrollee. Se l'utente seleziona "Start PIN", "Start PBC" o preme il pulsante fisico sull'apparato, il Router inizierà la ricerca di un Access Point WPS. Solo dopo aver avviato lo stesso metodo dal lato del registrar, si avvierà lo scambio del protocollo di registrazione per far si che il Router AP riceva il profilo wireless. Al termine il Router AP verrà associato ad un Access Point.

Istruzioni sull'impiego come AP e come Client

In questa fase, l' AP è trasparente per gli utenti. Se si vuole configurare una postazione o un qualsiasi dispositivo capace di operare come enrollee, deve digitare il PIN del dispositivo nel registrar esterno e selezionare il profilo wireless corretto. Dopo aver digitato il PIN, il registrar esterno comunicherà tale condizione all'AP. L'AP a sua volta provvederà a trasferire il profilo criptato dal registrar al dispositivo enrollee. Al termine, il dispositivo potrà utilizzare il profilo wireless ed associarsi all'AP. Si tenga però presente che il dispositivo potrebbe connettersi ad altri Access Point se il profilo wireless non appartiene anche al proxy AP. Si dovrà quindi prestare la massima attenzione nel selezionare o creare il profilo utente sul registrar esterno.

Pagina Wireless Advanced Settings

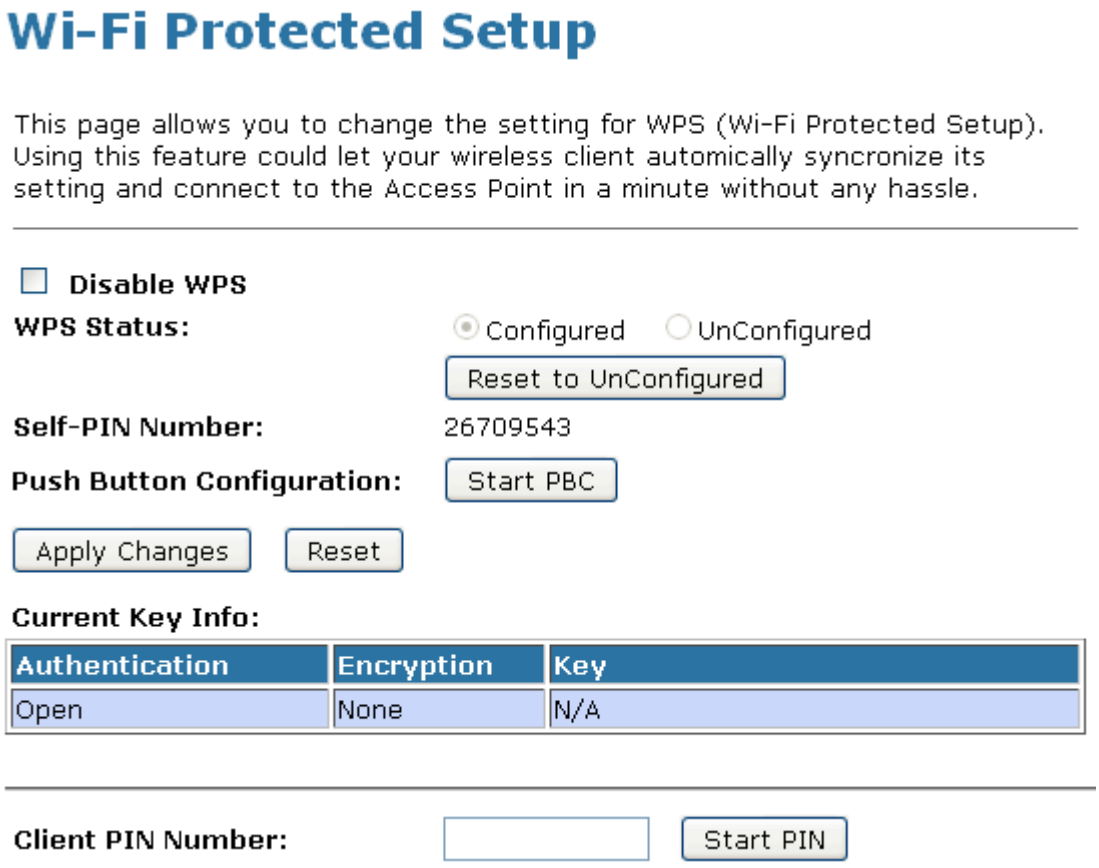
L'utente deve assicurarsi che il file “Broadcast SSID” sia abilitato. In caso contrario, il WPS potrebbe non funzionare correttamente.



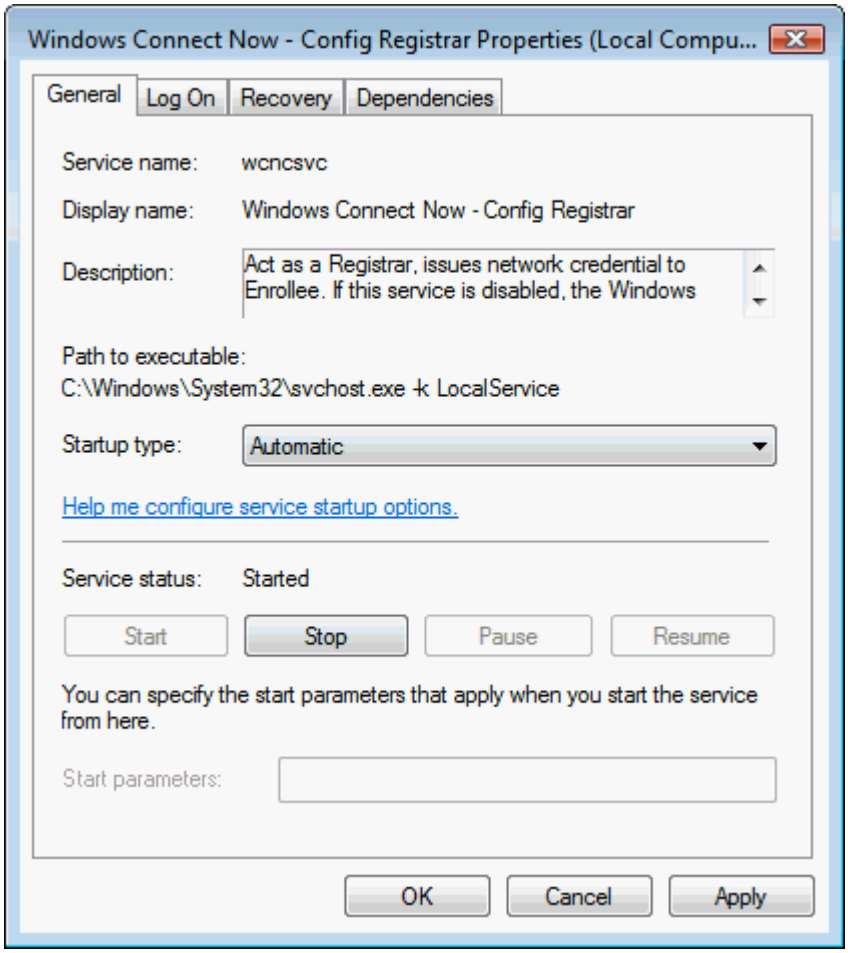
Impiego dell' AP come enrollee

In questo caso, l' AP sarà configurato da un qualunque registrar tramite EAP in banda o UPnP. L'utente non dovrà effettuare alcuna operazione dal lato AP, ma dovrà solamente digitare il PIN dell'AP nel Registrar. Si riporta di seguito un esempio per Vista WCN.

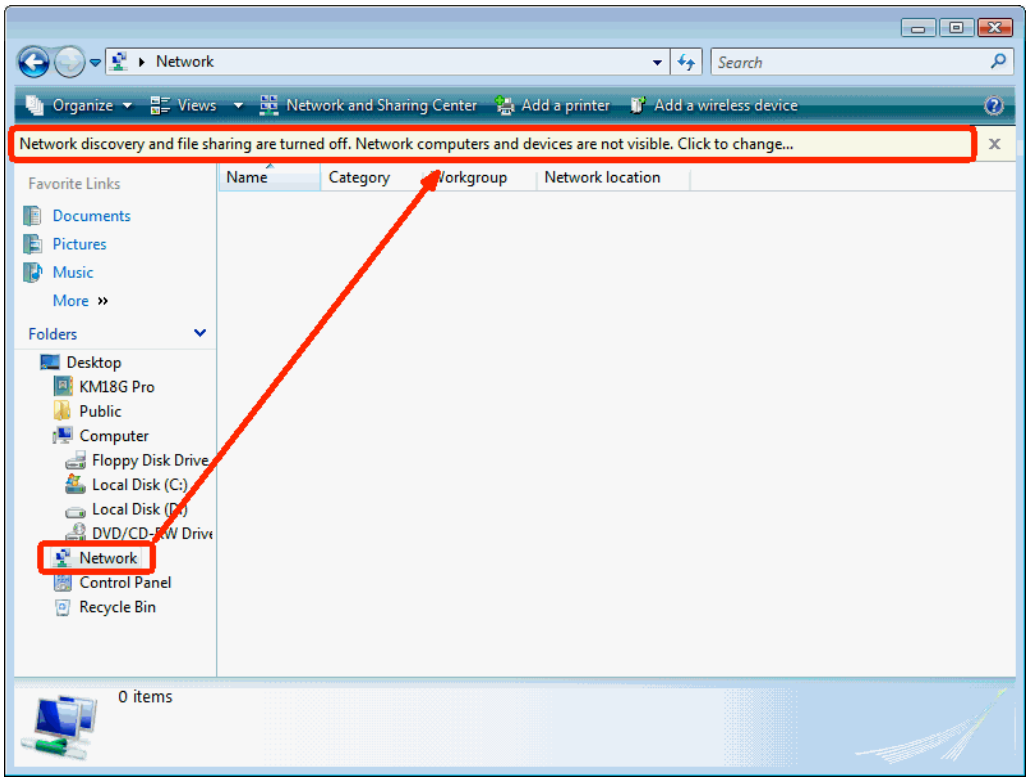
1. Dal menù di sinistra, selezionare *Wireless -> WPS*. Si visualizza la seguente pagina:
2. Assicurarsi che l' AP è in stato di 'non configurato' (UnConfigured).



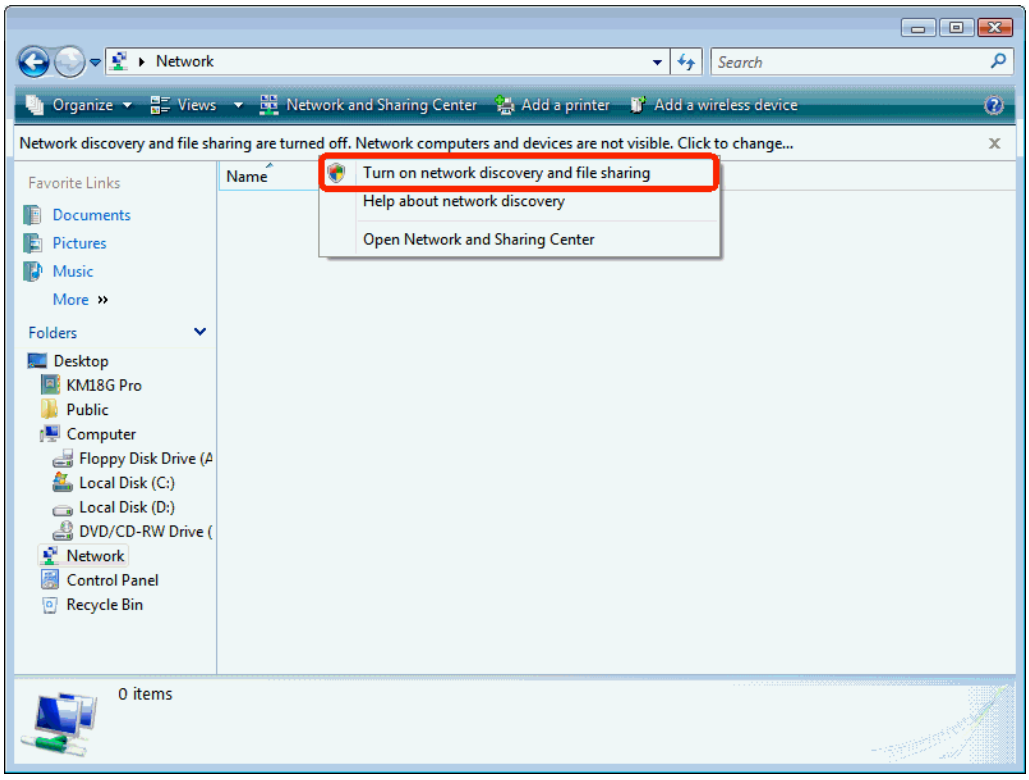
3. Collegare il cavo Ethernet nella porta LAN dell' AP ed assicurarsi che la connessione sia riconosciuta da Vista.
4. Assicurarsi che la funzione WCN sia abilitata. Potrebbe essere necessario abiltarlo la prima volta. A tale scopo:
   - aprire il “Pannello di Controllo” e selezionare “Vista Classica“,
   - aprire “Strumenti di Amministrazione”, fare doppio click su “Servizi” e, sulla finestra di Controllo Account Utente premere “Continua“,
   - configurare le proprietà della sezione "Windows Connect Now”,
   - selezionare il "Tipo di Startup” in Automatico e quindi premere “Start”.



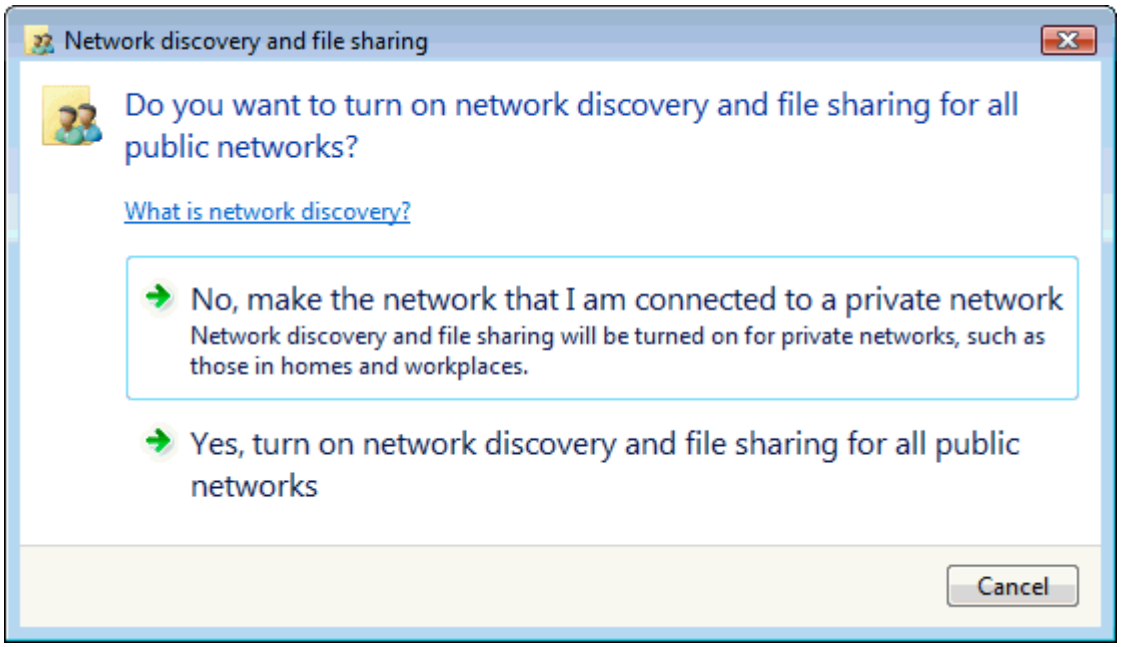
5. Al termine delle precedenti operazioni, aprire Windows Explorer ed andare alla sezione “Network”.
6. Cliccare con il mouse sul messaggio “Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to Change…“



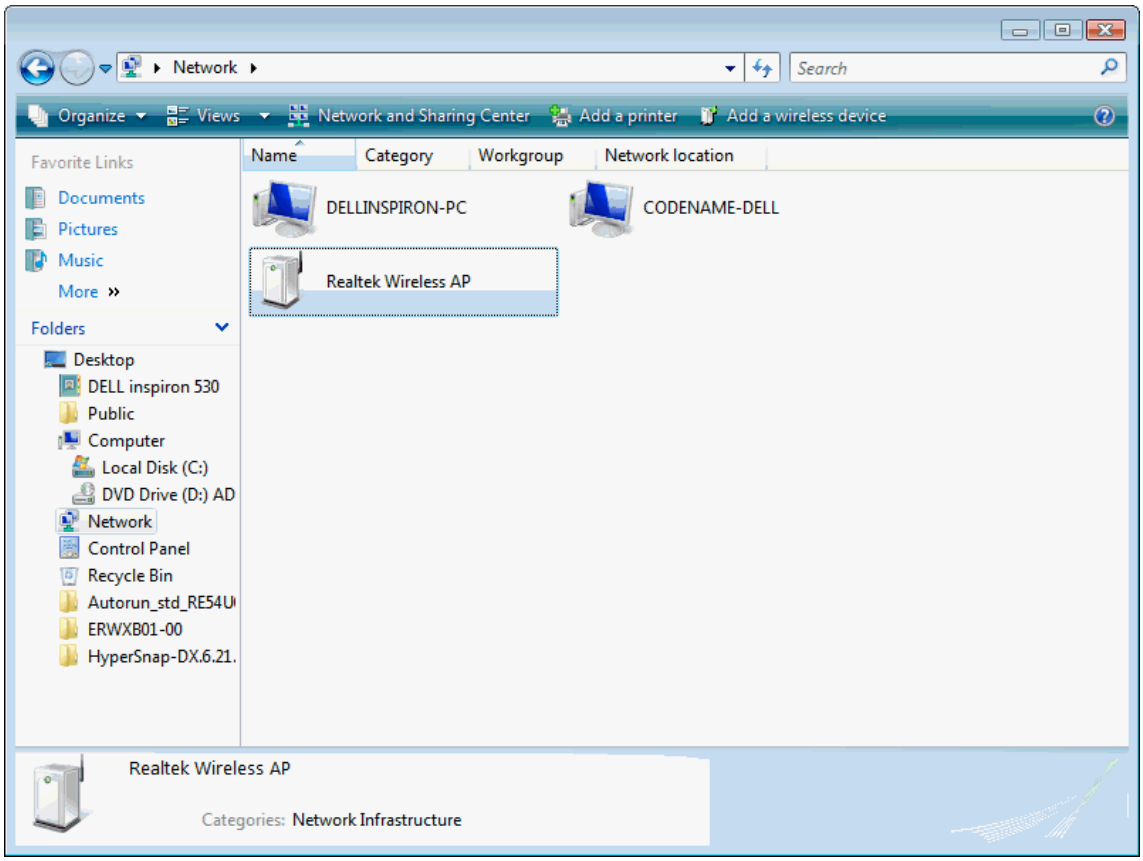
7. Selezionare “Turn on network discovery and file sharing“



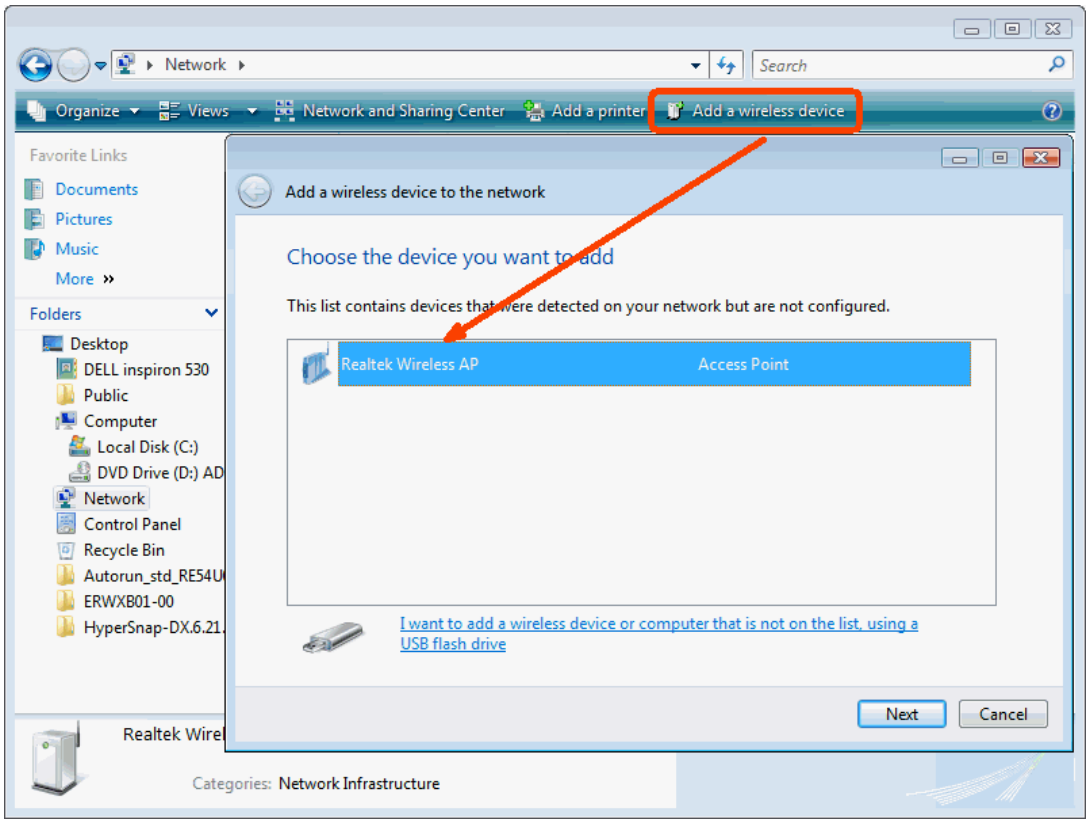
8. Selezionare “No, make the network that I am connected to a private network“


Network discovery and file sharing
Do you want to turn on network discovery and file sharing for all public networks?
What is network discovery?
No, make the network that I am connected to a private network
Network discovery and file sharing will be turned on for private networks, such as those in homes and workplaces.
Yes, turn on network discovery and file sharing for all public networks
Cancel

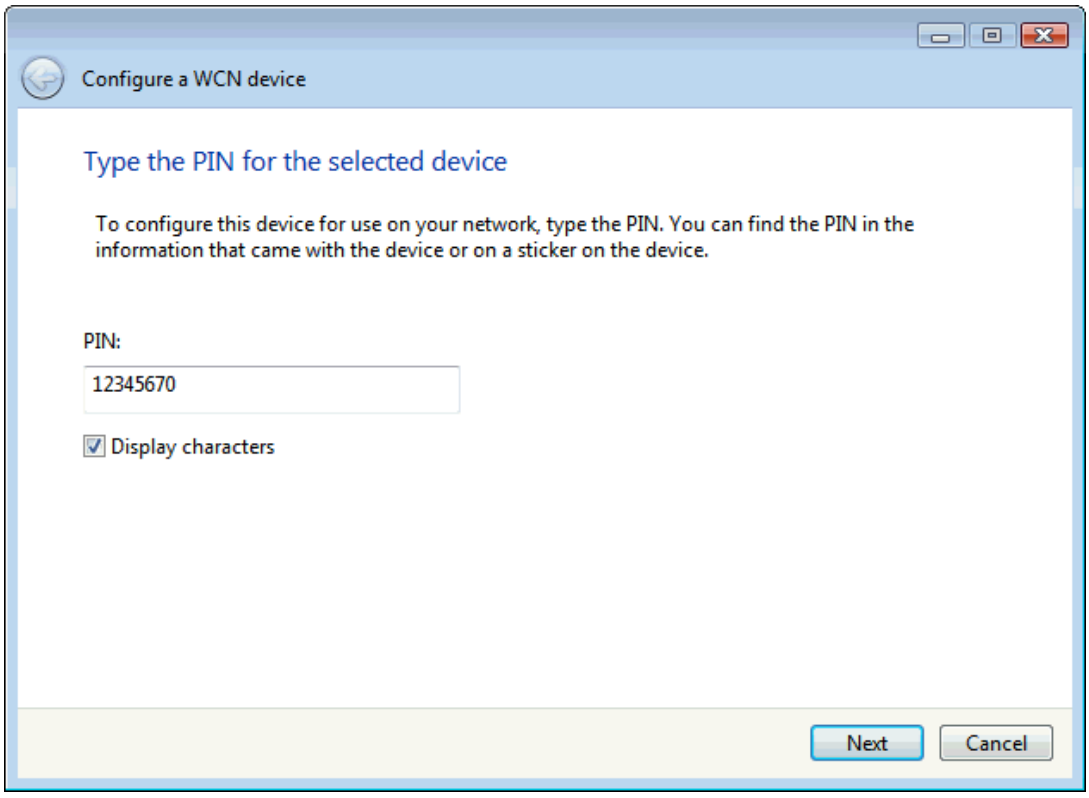
9. Verra visualizzata l'icona del Router AP. Fare doppio click su di essa.



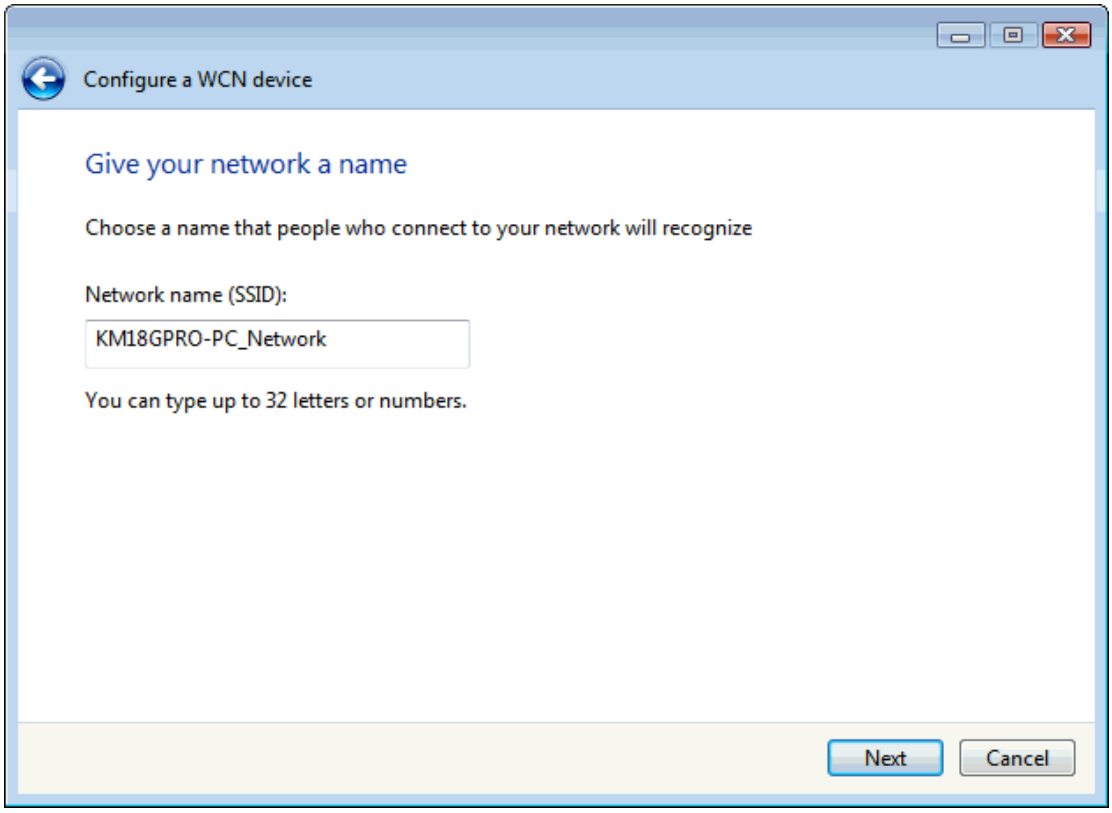
10. Se l'icona non viene visualizzata, si può anche selezionare “Add a wireless device” e premere “next”.



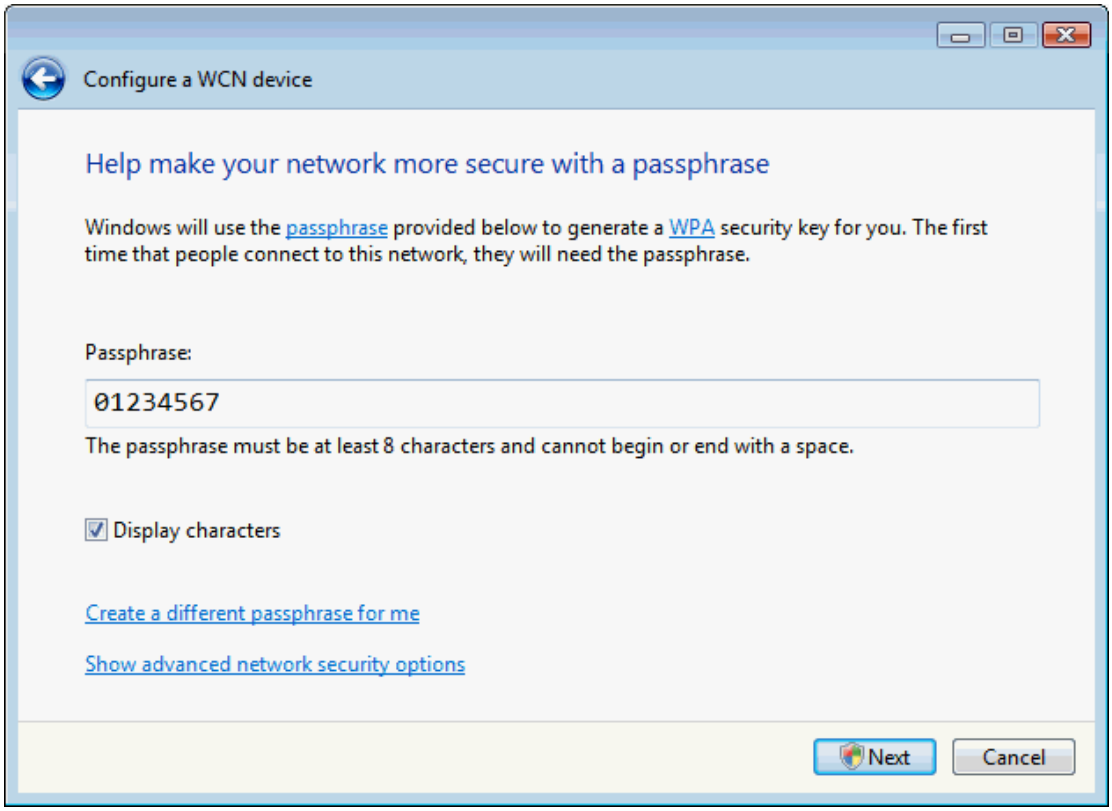
11. Digitare il Self-PIN Number dell'AP e premere “next”.


Configure a WCN device
Type the PIN for the selected device
To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.
PIN:
12345670
Display characters
Next
Cancel

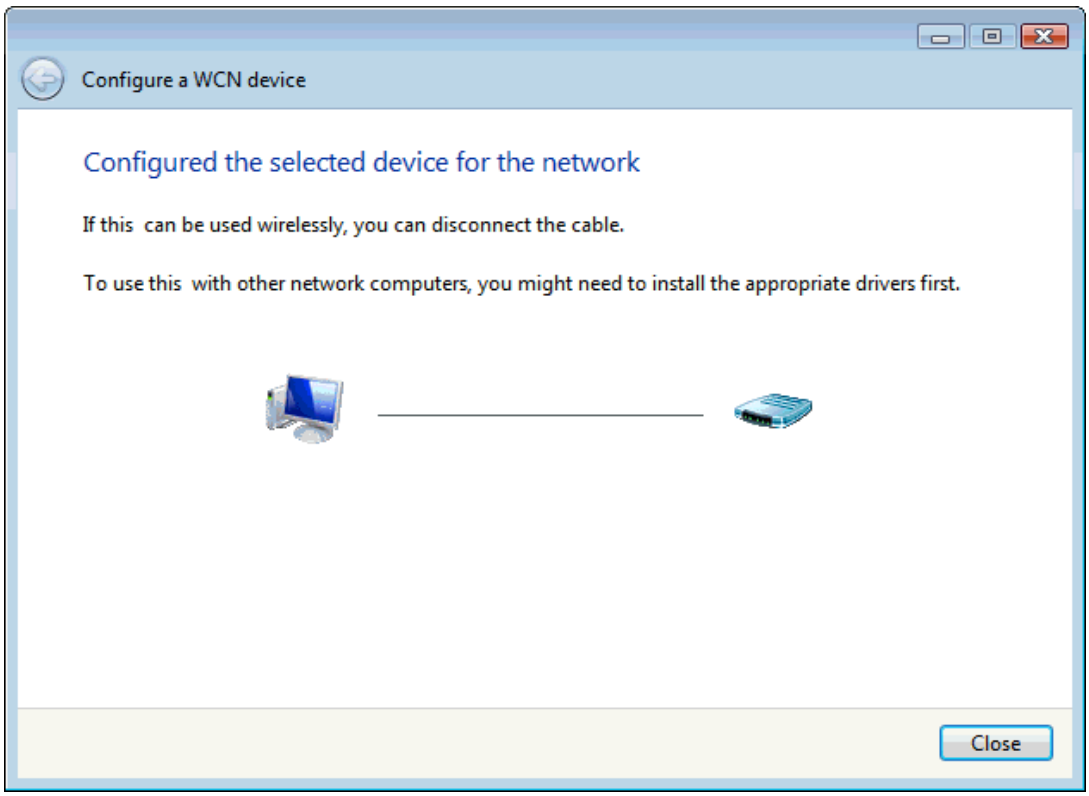
12. Scegliere un nome per la rete che possa essere facilmente riconosciuto degli utenti che si collegano alla rete.


Configure a WCN device
Give your network a name
Choose a name that people who connect to your network will recognize
Network name (SSID):
KM18GPRO-PC_Network
You can type up to 32 letters or numbers.
Next
Cancel

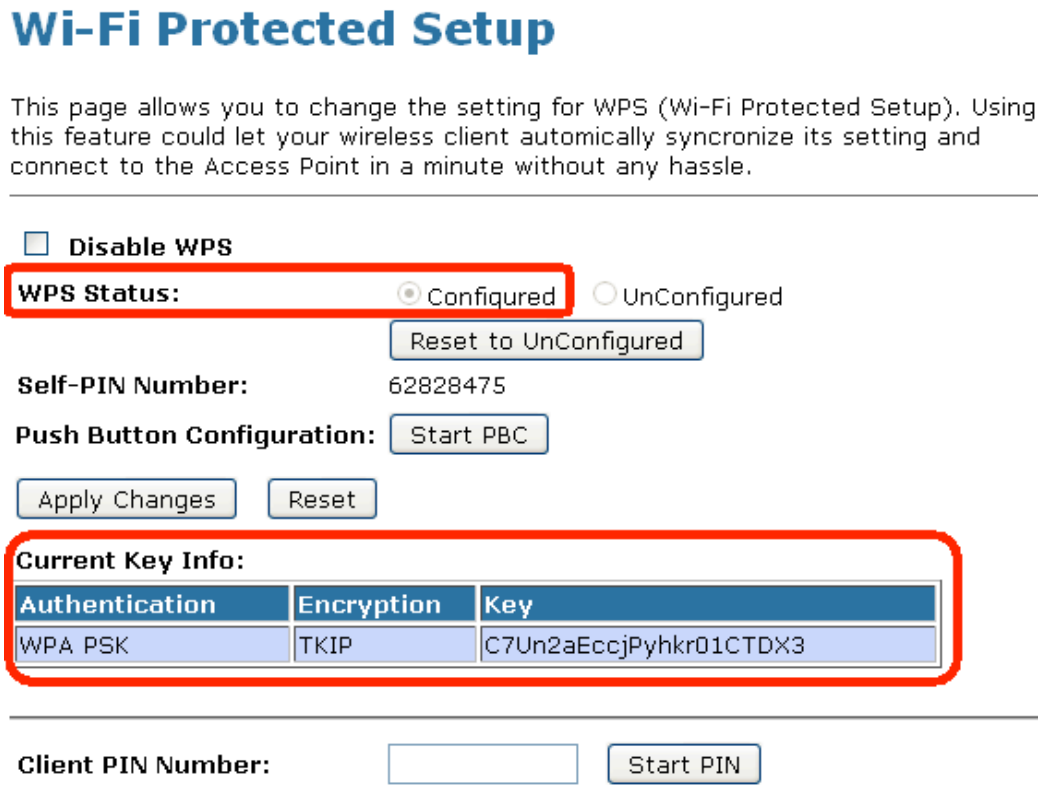
13. Digitare la Passphrase e quindi premere Next.


Configure a WCN device
Help make your network more secure with a passphrase
Windows will use the passphrase provided below to generate a WPA security key for you. The first time that people connect to this network, they will need the passphrase.
Passphrase:
01234567
The passphrase must be at least 8 characters and cannot begin or end with a space.
Display characters
Create a different passphrase for me
Show advanced network security options
Next
Cancel

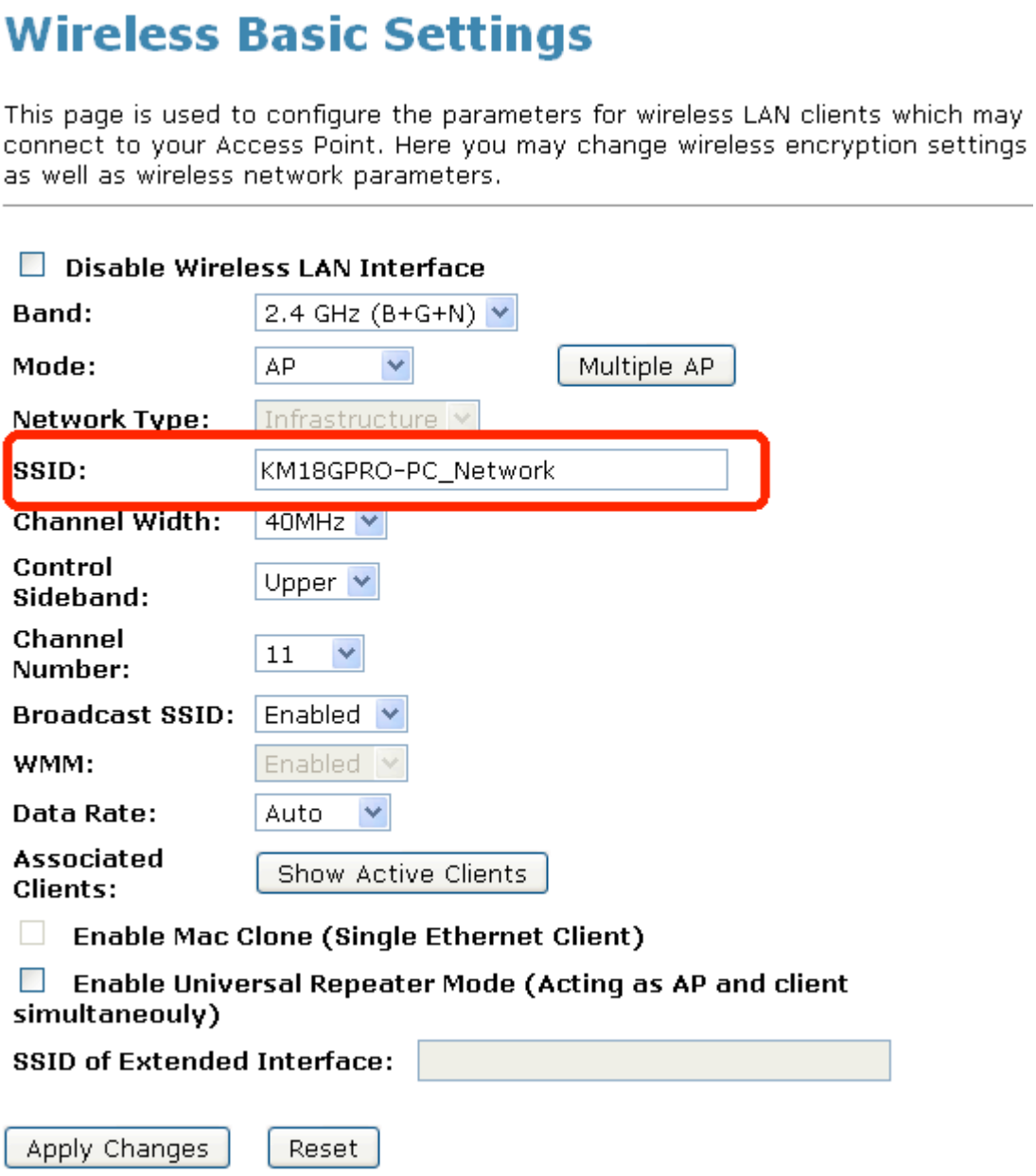
14. Verrà visualizzato una finestra di controllo dell'Account Utente e quindi premere Continue.
15. Al termine il Router AP è stato correttamente configurato dal WCN.


Configure a WCN device
Configured the selected device for the network
If this can be used wirelessly, you can disconnect the cable.
To use this with other network computers, you might need to install the appropriate drivers first.
Close

16. Alla fine l'AP assumerà lo stato di "Configurato" (si veda il WPS Status). L'algoritmo di autenticazione, l'algoritmo di cifratura e la chiave assegnata dal WCN saranno visibili nella sezione "Current Key Info".


Wi-Fi Protected Setup
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.
Disable WPS
WPS Status: Configured UnConfigured
Reset to UnConfigured
Self-PIN Number: 62828475
Push Button Configuration: Start PBC
Apply Changes Reset
Current Key Info:
Authentication Encryption Key
WPA PSK TKIP C7Un2aEccjPyhkr01CTDX3
Client PIN Number: Start PIN

17. Il campo SSID della pagina Wireless Basic Settings sarà anch'esso reimpostato al valore assegnato dal WCN.



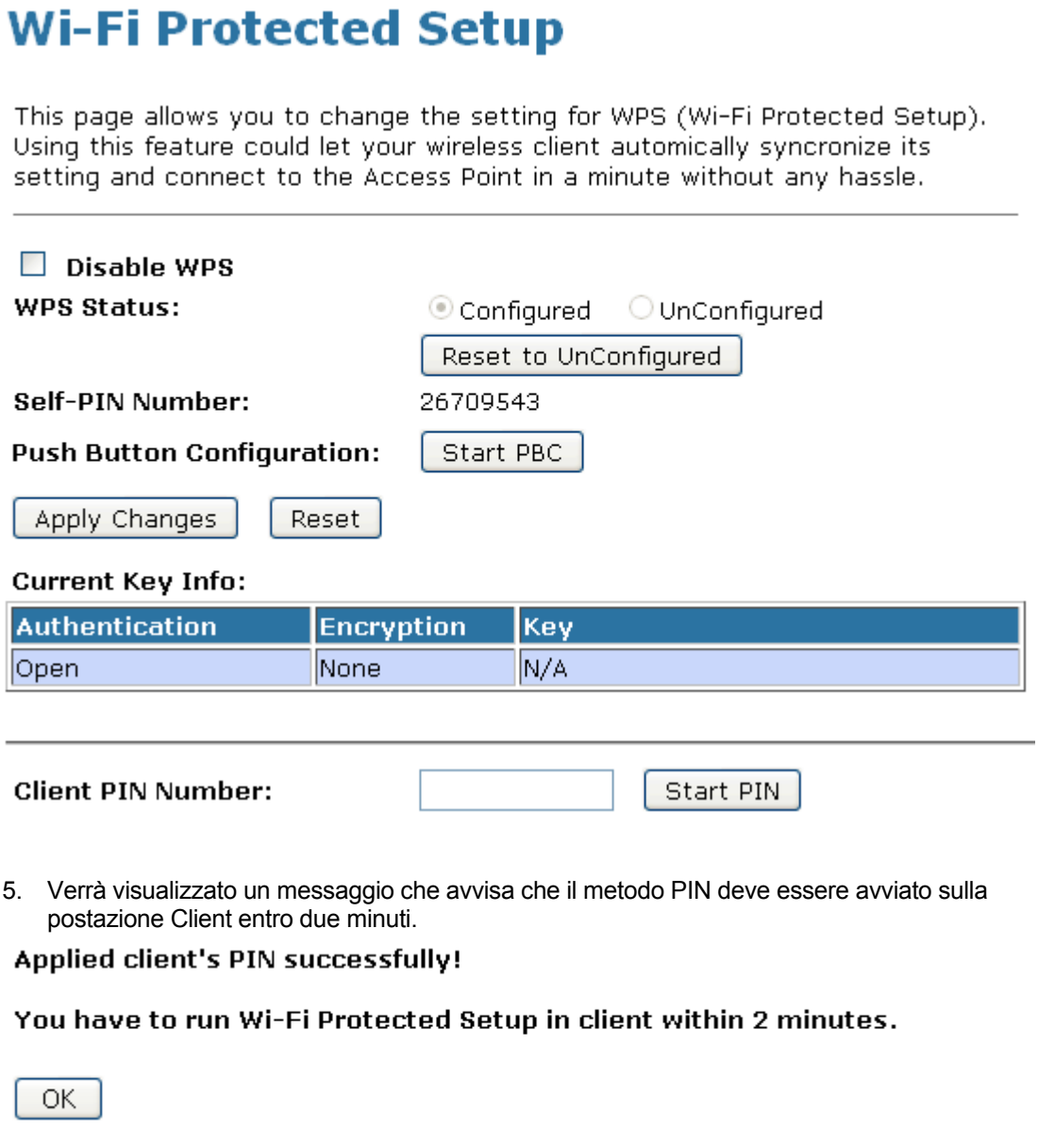
18. Analogamente, anche la configurazione della sicurezza visibile dalla pagina Wireless Security sarà aggiornata ai valori inviati dal WCN. Se l'utente cercasse di modificare i valori della sicurezza, verrebbe generato un messaggio di warning. Il motivo di questo è già stato descritto nella sezione precedente.

Impiego dell' AP come registrar

Modalità AP

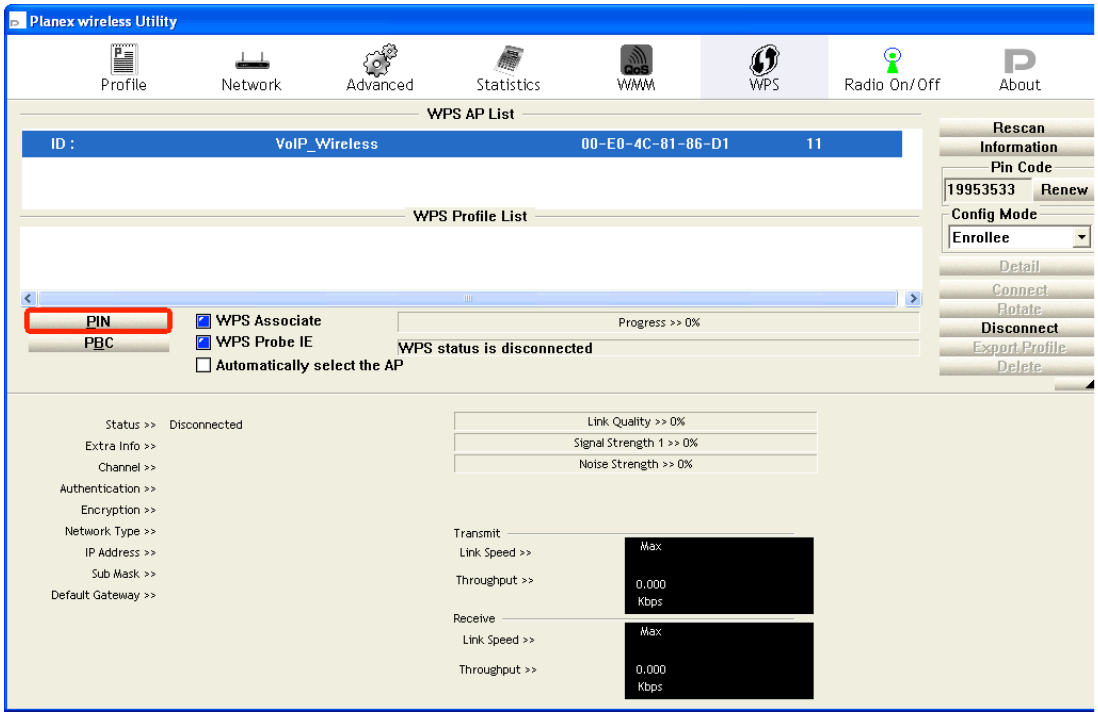
Ogni volta che l'utente digita il PIN di una postazione nella pagina Wi-Fi Protected Setup e seleziona "Start PIN", l' AP diventa un registrar. Il metodo PIN deve essere avviato sulla postazione entro due minuti.

1. Dal menù di sinistra, selezionare *Wireless -> WPS*. Si visualizza la seguente pagina:
2. Assicurarsi che l' AP è in stato di non-configurato (UnConfigured).
3. Digitare il numero PIN del Client.
4. Premere *Start PIN*.

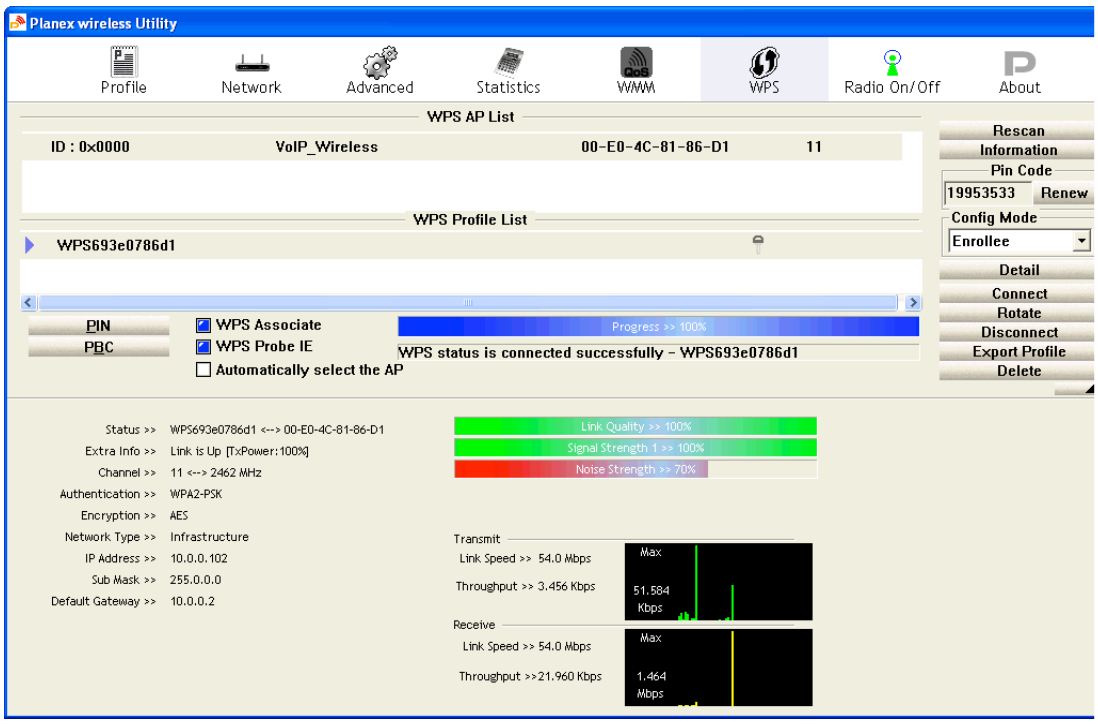


5. Verrà visualizzato un messaggio che avvisa che il metodo PIN deve essere avviato sulla postazione Client entro due minuti.

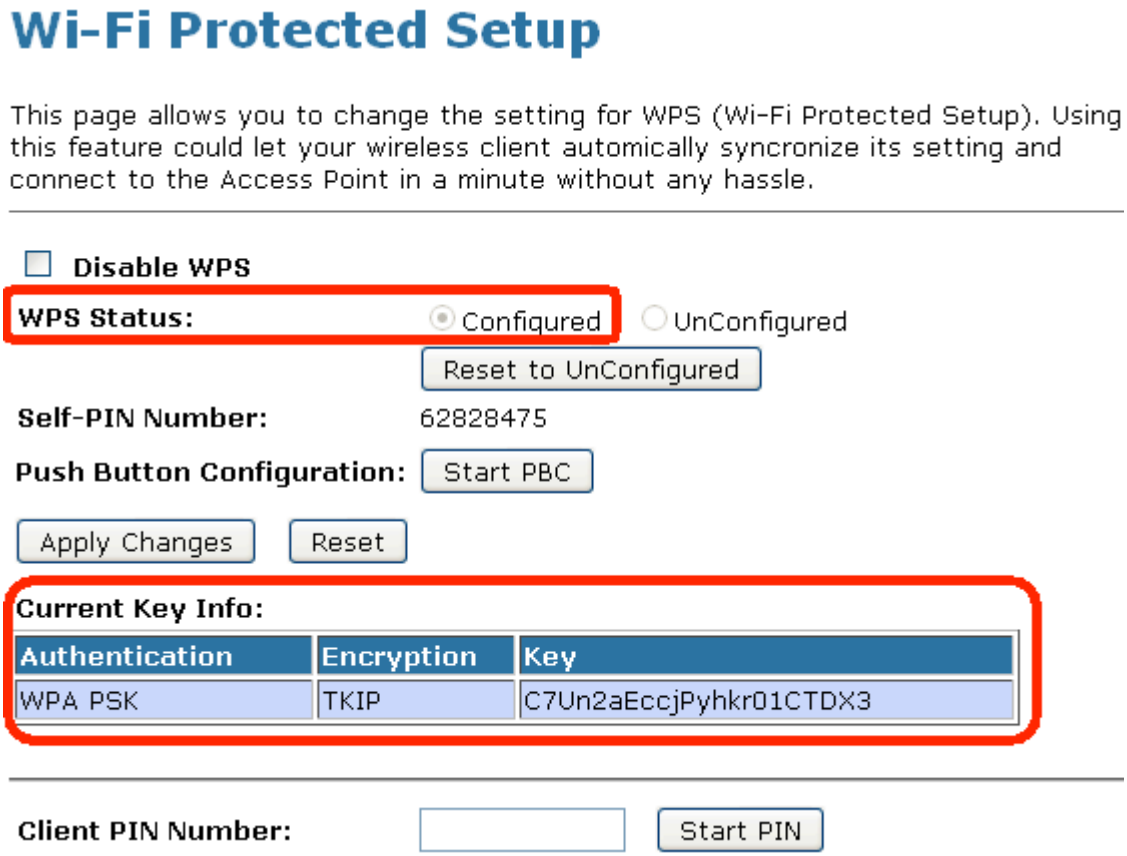
6. Dal lato della postazione, si dovrà avviare il metodo PIN entro due minuti.



7. Se il PIN del dispositivo è corretto e lo scambio messaggi WPS con la postazione avviene correttamente, lo stato di User's Wi-Fi Protected sarà visualizzato come di seguito.



8. Analogamente, dal lato AP, se il PIN del dispositivo è corretto e lo scambio messaggi WPS con la postazione avviene correttamente la pagina AP's Wi-Fi Protected Setup sarà visualizzata come di seguito.



Le restanti pagine quali *Wireless Basic Settings* e *Wireless Security Setup* saranno aggiornate opportunamente come descritto nella precedente sezione. L' AP resterà nello stato di "non configurato" finché la postazione non inizia lo scambio di messaggi WPS. Conformemente alle specifiche WPS, durante lo scambio di messaggi WPS, l' AP creerà un profilo wireless con modalità WPA2-mixed ed una chiave generata in modo casuale.

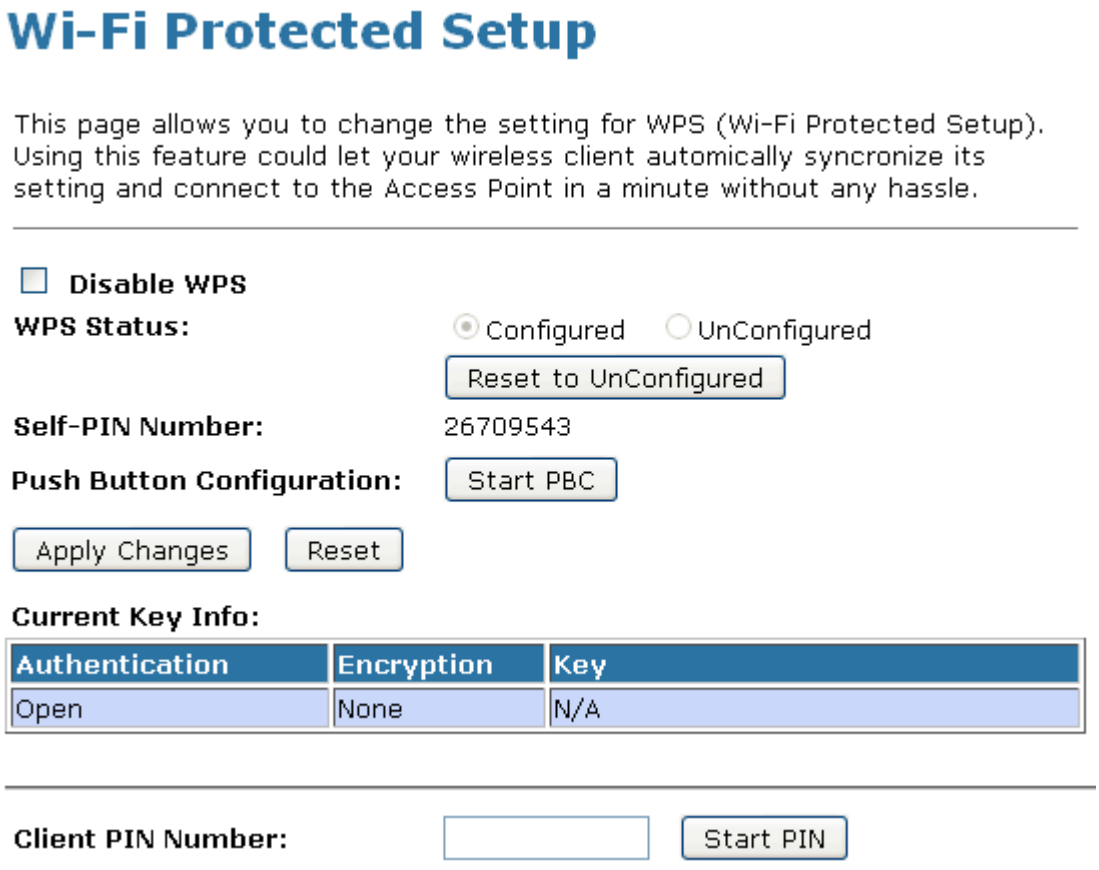
Si noti che, qualora l'AP fosse già nello stato di "configurato", l'AP utilizzerà il profilo wireless originale, fornendolo alla postazione. Ciò significa che tutte le configurazioni dell'AP non cambieranno e che tutte le pagine relative al WPS rimarranno le stesse.

Metodo Push Button

Il Router AP supporta un pulsante virtuale, denominato “Start PBC” e presente nella pagina Wi-Fi Protected Setup, per il metodo Push Button. Se si preme il pulsante virtuale “Start PBC”, l'AP inizierà una sessione WPS e rimarrà in attesa di una qualsiasi postazione che si voglia unire alla rete. Allo stato attuale, l' AP potrebbe rilevare la presenza di più postazioni che abbiano avviato il metodo PBC. In presenza di più sessioni PBC, si consiglia di provare con il metodo PIN.

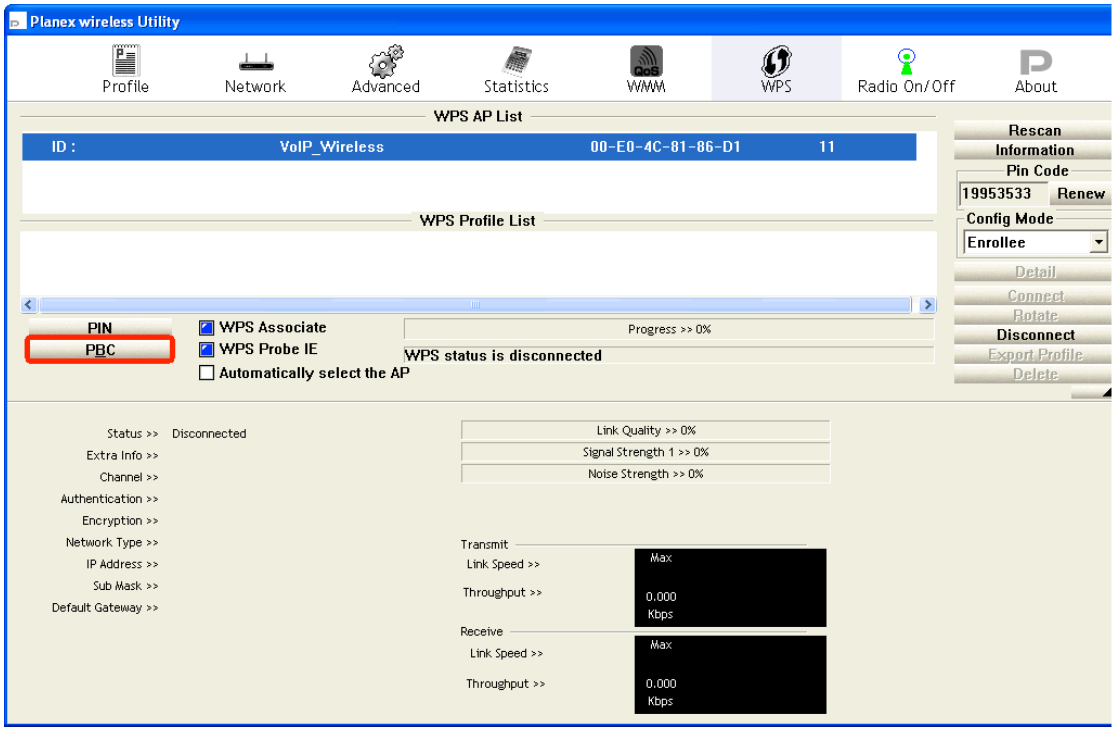
Dopo che siè premuto il pulsante virtuale “Start PBC” dell'AP, si dovrà premere il relativo pulsante della postazione entro due minuti. Se il WPS è stato eseguito correttamente, l' AP ha fornito il proprio profilo wireless alla postazione e questa potrà usare tale profilo per associarsi all' AP.

1. Dal menù di sinistra, selezionare *Wireless -> WPS*. Si visualizza la seguente pagina:
2. Assicurarsi che l' AP è in stato di non-configurato (UnConfigured).
3. Premere *Start PBC*.

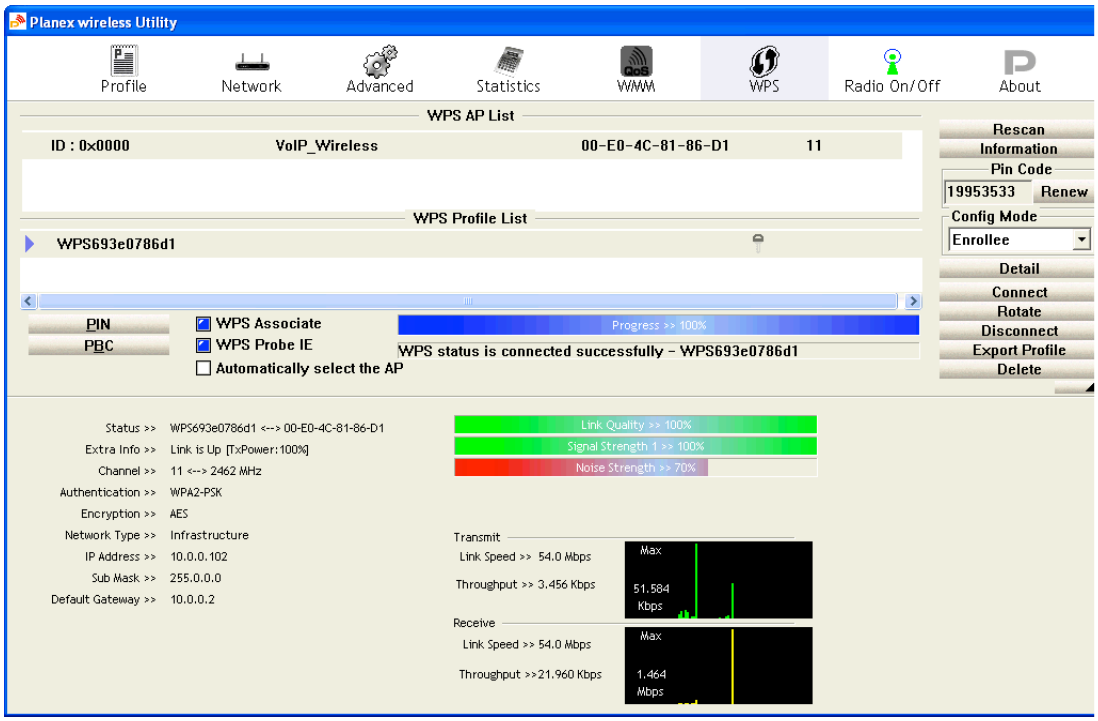


4. Verrà visualizzato un messaggio che avvisa che il metodo PBC deve essere avviato sulla postazione entro due minuti.

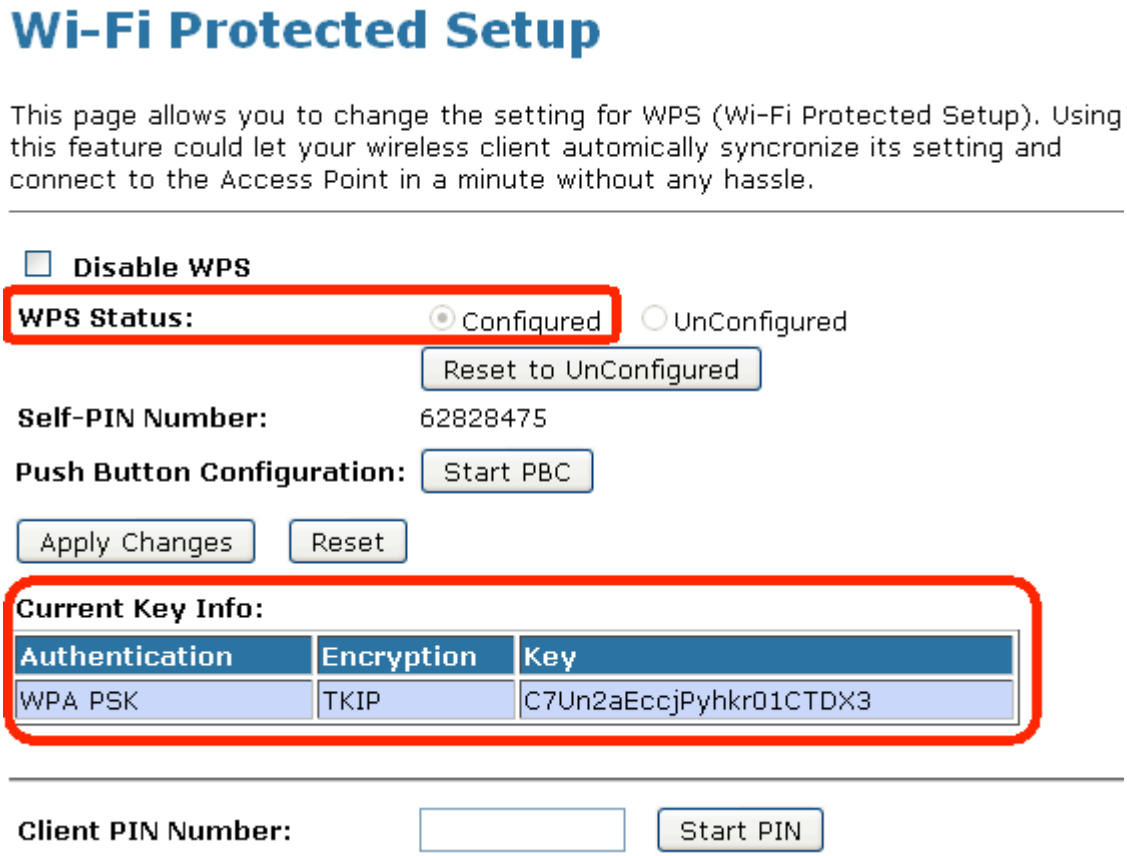
5. Dal lato della postazione, si dovrà avviare il metodo PCB entro due minuti.



6. Se il PIN del dispositivo è corretto e lo scambio messaggi WPS con la postazione avviene correttamente, lo stato di User's Wi-Fi Protected sarà visualizzato come di seguito.



7. Analogamente, dal lato AP, se il PIN del dispositivo è corretto e lo scambio messaggi WPS con la postazione avviene correttamente la pagina AP's Wi-Fi Protected Setup sarà visualizzata come di seguito.



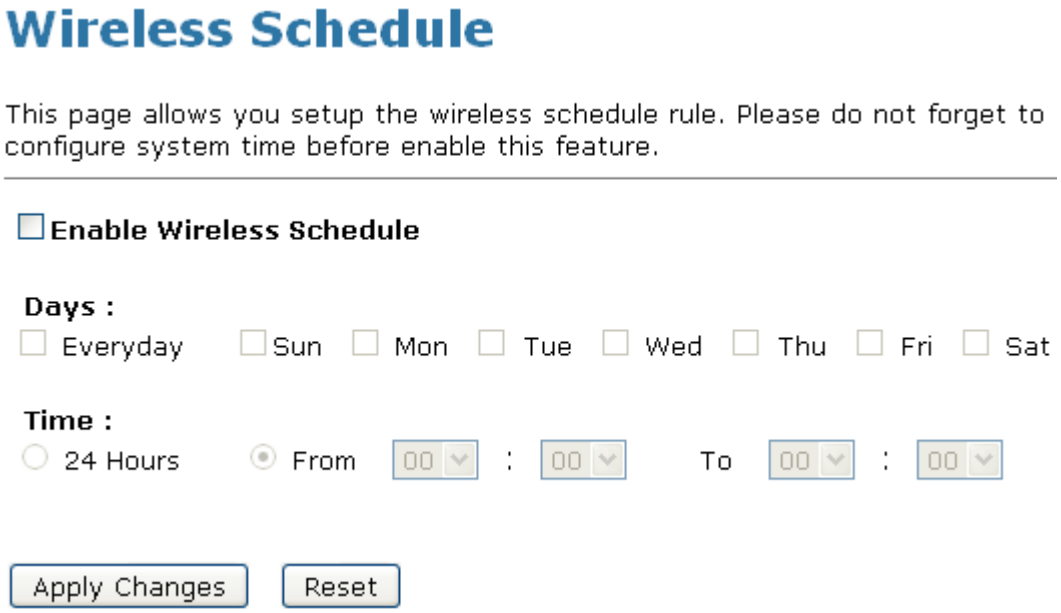
Le restanti pagine quali *Wireless Basic Settings* e *Wireless Security Setup* saranno aggiornate opportunamente come descritto nella precedente sezione. L' AP resterà nello stato di "non configurato" finché la postazione non inizia lo scambio di messaggi WPS. Conformemente alle specifiche WPS, durante lo scambio di messaggi WPS, l' AP creerà un profilo wireless con modalità WPA2-mixed ed una chiave generata in modo casuale.

Si noti che, qualora l'AP fosse già nello stato di "configurato", l'AP utilizzerà il profilo wireless originale, fornendolo alla postazione. Ciò significa che tutte le configurazioni dell'AP non cambieranno e che tutte le pagine relative al WPS rimarranno le stesse.

Scheduling della rete Wireless

Questa pagina permette di configurare le regole per la pianificazione delle attività della rete wireless. Prima di procedere assicurarsi che l'orologio di sistema sia aggiornato. Per accedere alla pagina *Wireless Schedule* :

Dal menù *Wireless* di sinistra selezionare *Wireless Schedule*. Si visualizza la seguente pagina:


Wireless Schedule
This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.
Enable Wireless Schedule
Days :
Everyday Sun Mon Tue Wed Thu Fri Sat
Time :
24 Hours From 00 : 00 To 00 : 00
Apply Changes
Reset

10 Interfaccia LAN

Il presente capitolo descrive come configurare i parametri della rete locale connessa alla porta LAN del dispositivo. In tale fase è possibile modificare parametri quali l'indirizzo IP, la Subnet Mask, il DHCP, ecc...

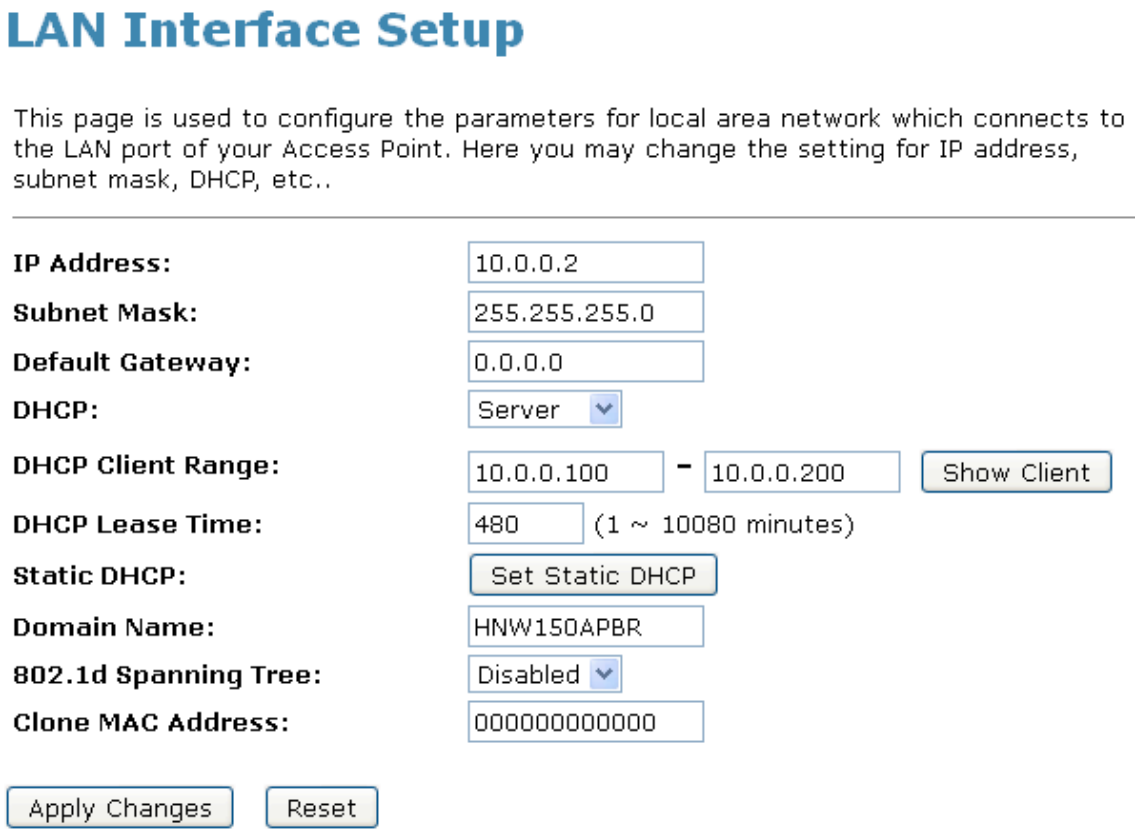
Nota

La modifica dei parametri di indirizzamento potrebbe essere necessaria per specifica richiesta dell'ISP oppure potrebbe essere una scelta per chi è esperto delle configurazioni di rete. Nella maggior parte dei casi, non vi è necessità di cambiare i parametri preimpostati.

Setup della interfaccia LAN

Per verificare la configurazione della interfaccia LAN:

1. Dal menu di sinistra selezionare *Network Settings -> LAN Interface*. Si visualizza la seguente pagina:

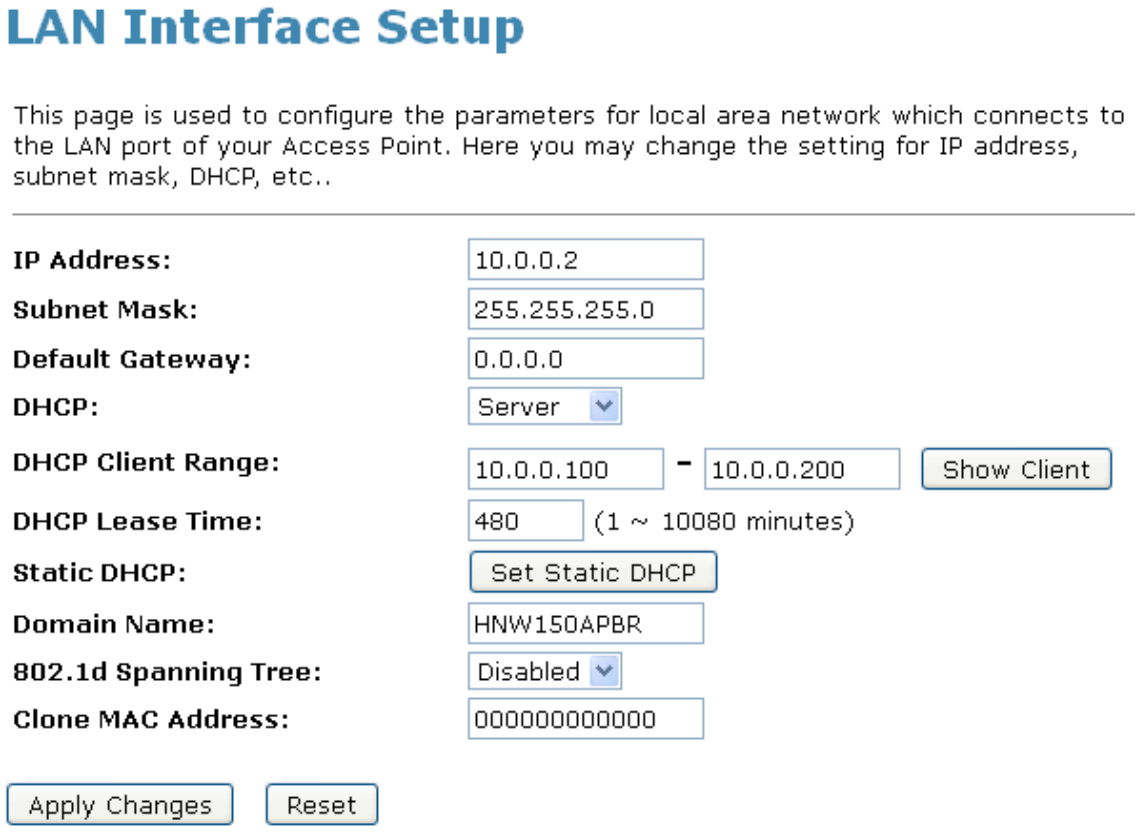


Campo	Descrizione
IP Address	L'indirizzo IP della LAN Default: 10.0.0.2
Subnet Mask	La Subnet Mask della LAN Default: 255.255.255.0
Default Gateway	Il Gateway di Default della LAN Default: 0.0.0.0
DHCP	Tipo di DHCP: Disabilitato, DHCP Client o Server Default: DHCP Server
DHCP Client Range	Definisce l'indirizzo IP iniziale e finale del set di indirizzi IP validi Default IP iniziale: 10.0.0.100 Default IP finale: 10.0.0.200
Show Client	I computer o i dispositivi DHCP client collegati all'apparato saranno visualizzati nella tabella dei DHCP Client, mostrando le proprie informazioni di identificazione. Per ciascun computer / dispositivo, la tabella visualizzerà l'indirizzo IP, il MAC Address e il tempo di validità (Expired Time) dell'indirizzo IP assegnato.
Domain Name	Il Domain Name (nome del dominio) si usa per identificare in modo più semplice l'indirizzo IP ad esso associato. Il Domain Name deve essere unico; la loro assegnazione è controllata dalla Internet Corporation for Assigned Names and Numbers (ICANN). I Domain name sono gli elementi chiave per gli URL, ossia gli indirizzi che identificano un file specifico su un sito web.
802.1d Spanning Tree	Abilita o disabilita lo Spanning Tree
Clone MAC Address	Duplicazione del MAC Address su LAN Default: 000000000000

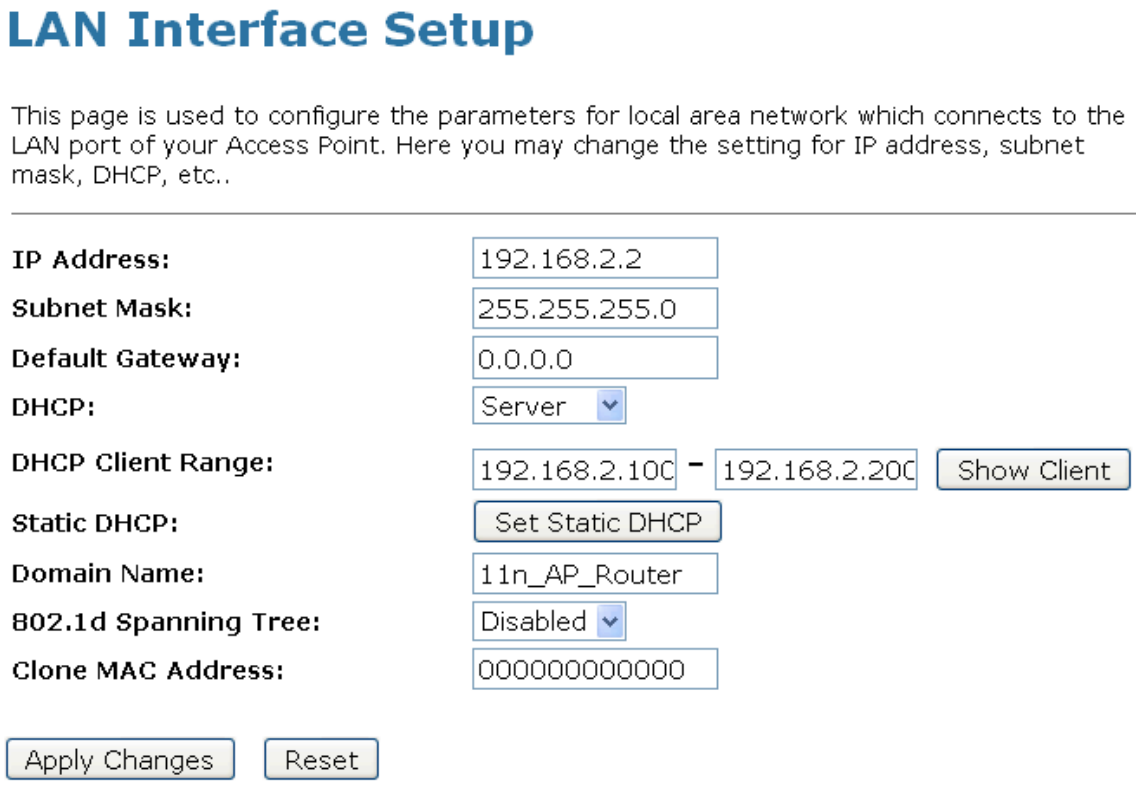
Cambio Indirizzo IP e Subnet Mask della LAN

Per verificare la configurazione della interfaccia LAN:

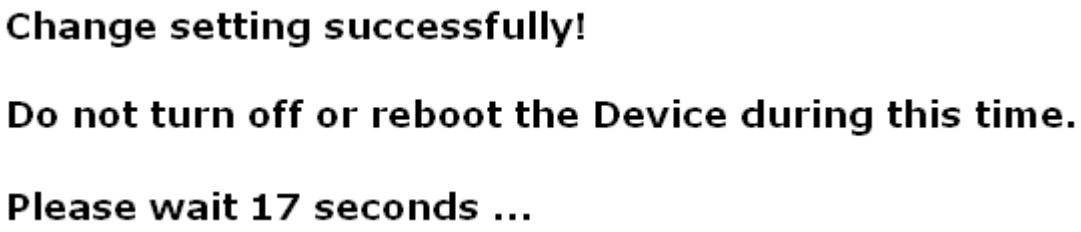
2. Dal menu di sinistra selezionare *Network Settings -> LAN Interface*. Si visualizza la seguente pagina:



3. Digitare l'indirizzo IP e selezionare *Change default LAN port IP address*.
4. Nei campi *IP Address* e *Subnet Mask* digitare il nuovo indirizzo IP e la relativa Subnet Mask.
5. Cambiare il range di default del Client DHCP.
6. Premere il pulsante *Apply Changes*.



7. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Attendere 20 secondi…



Potrebbe essere anche necessario rinnovare l'assegnazione degli indirizzi del DHCP:

Windows 95/98

a. Selezionare **Run**... (Esegui) dal menù **Start**.

b. Digitare **winipcfg** e premere **OK**.

c. Selezionare la scheda di rete dall'elenco predefinito

d. Premere prima **Release All** e successivamente **Renew All**.

e. Uscire (**Exit**) dal programma winipcfg.

Windows NT/Windows 2000/Windows XP

a. Aprire una finestra del **Prompt dei comandi**.

b. Digitare **ipconfig /release** nella finestra dei comandi.

c. Digitare quindi **ipconfig /renew**.

d. Digitare **exit** per chiudere la finestra del Prompt dei comandi.

Linux

a. Attivare una shell.

b. Digitare **pump -r** per rilasciare l'assegnazione degli indirizzi.

c. Digitare **pump** per rinnovare l'assegnazionedegli indirizzi.

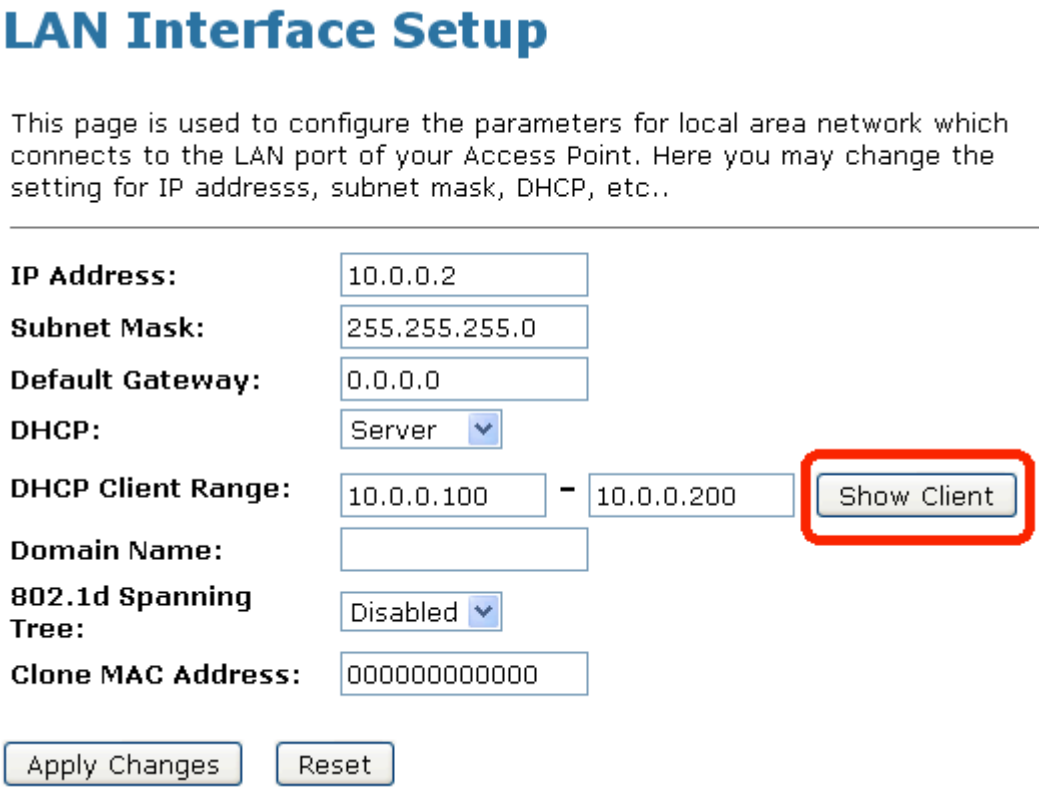
Nota

Se si cambia l'indirizzo IP del dispositivo mentre è collegato tramite il browser WEB, questo verrà automaticamente disconnesso. E' necessario reinserire il nuovo indirizzo IP come URL di destinazione per ricollegarsi alle pagine di configurazione del dispositivo.

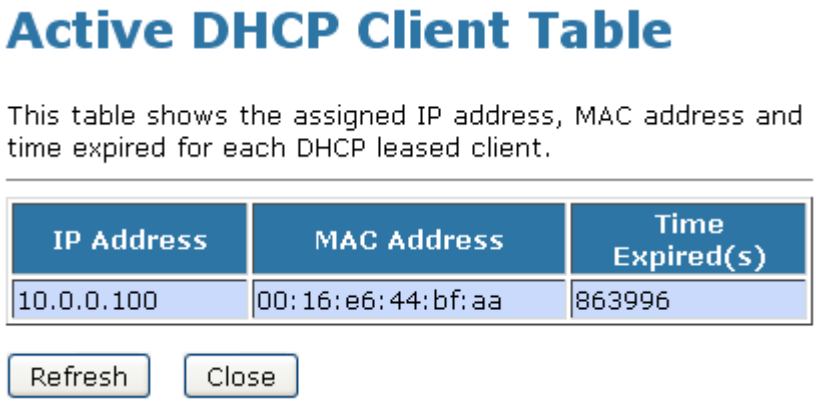
Show Client

Per controllare l'indirizzo IP, il MAC Address ed il tempo di validità di ciascun computer/dispositivo collezionato nel DHCP:

1. Dal menu di sinistra selezionare *Network Settings -> LAN Interface*. Si visualizza la seguente pagina:



2. Premere il pulsante *Show Client*. Si visualizza la seguente pagina:



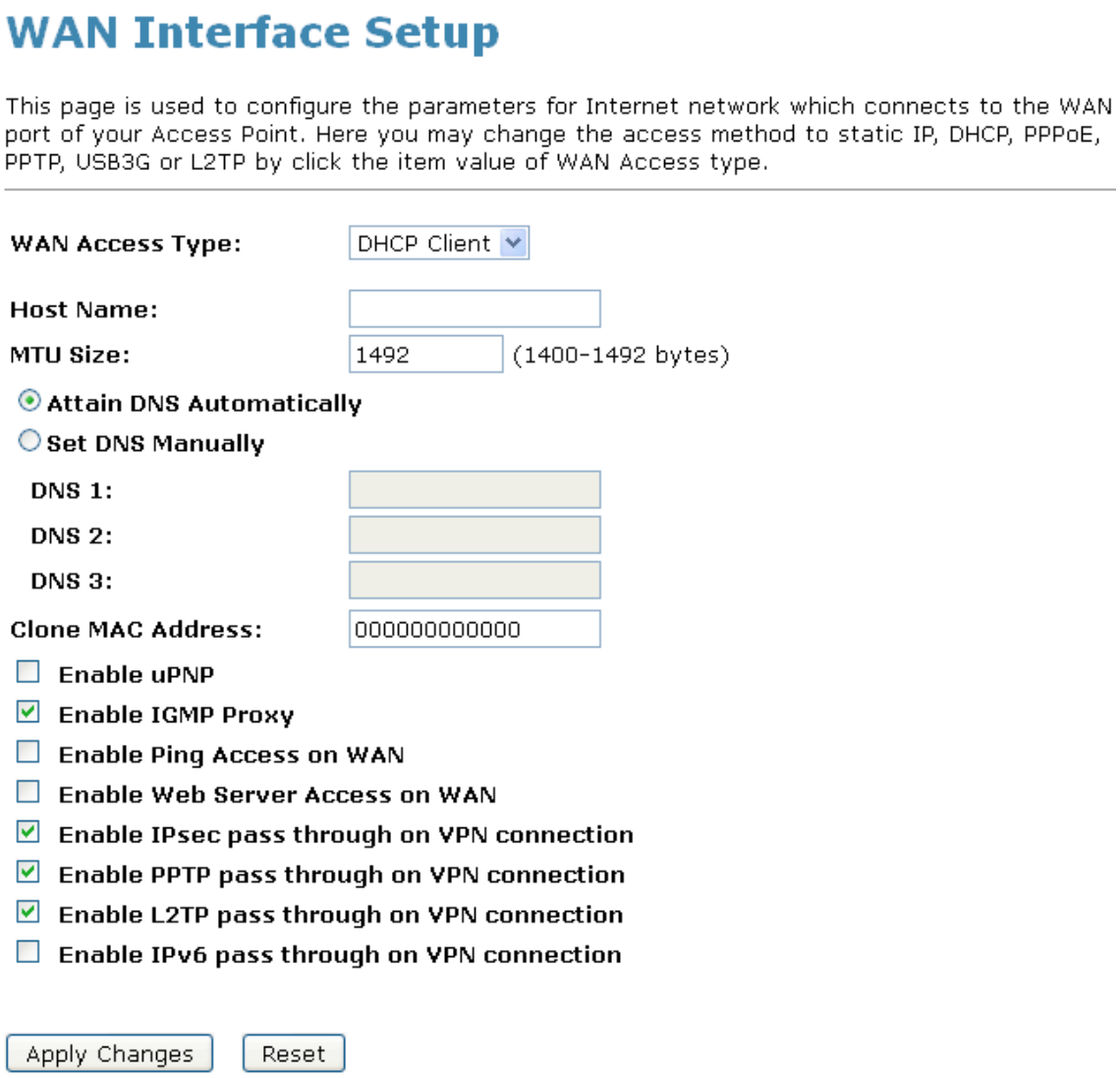
11 Interfaccia WAN

Il presente capitolo descrive come configurare la modalità con cui il dispositivo si connette ad Internet. Il vostro ISP (Internet Service Provider) determina il tipo di accesso Internet di cui si dispone, fornendo tutte le informazioni richieste per configurare l'accesso Internet sul dispositivo.

Il Router supporta quattro metodi per ottenere l'indirizzo IP per la connessione WAN:

Opzioni	Descrizione
Static IP	Selezionare questa opzione qualora la linea in uso sia assegnata con un indirizzo IP fisso.
DHCP Client	Selezionare questa opzione se la connessione ad Internet si realizza attraverso un Modem di linea.
PPPoE	Selezionare questa opzione se la connessione ad Internet si realizza attraverso una linea DSL
PPTP	Selezionare questa opzione se la connessione ad Internet si realizza attraverso un Server PPTP
L2TP	Selezionare questa opzione se la connessione ad Internet si realizza attraverso un Server L2TP

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*. Si visualizza la seguente pagina:


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Host Name:
MTU Size:
1492
(1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Enable IPv6 pass through on VPN connection
Apply Changes
Reset

Opzione		Descrizione
WAN Access Type	Static IP	Selezionare questa opzione qualora la linea in uso sia assegnata con un indirizzo IP fisso.
	DHCP Client	Selezionare questa opzione se la connessione ad Internet si realizza attraverso un Modem di linea.
	PPPoE	Selezionare questa opzione se la connessione ad Internet si realizza attraverso una linea DSL
	PPTP	Selezionare questa opzione se la connessione ad Internet si realizza attraverso un Server PPTP
	L2TP	Selezionare questa opzione se la connessione ad Internet si realizza attraverso un Server L2TP
Host Name		Il nome dell'host DHCP
IP Address		Verificare con quanto fornito dal vostro provider ISP
Subnet Mask		Verificare con quanto fornito dal vostro provider ISP
Default Gateway		Verificare con quanto fornito dal vostro provider ISP
User Name		Nomne utente per la registrazione PPPoE, fornito dall' Internet service provider
Password		Password per la registrazione PPPoE, fornita dall' Internet service provider
Service Name		Service Name per la registrazione PPPoE, fornita dall' Internet service provider
Connection Type	Continuous	La connessione è sempre attiva
	Connect on Demand	Inserire i minuti di connessione oltre i quali la sessione deve disconnettersi, se non si è verificata attività
	Manual	Connesso manualmente
Idle Time		Inserire i minuti di connessione oltre i quali la sessione deve disconnettersi
WAN Physical		IP dinamico o IP statico per connessione PPP
MTU Size		Specifica il rapporto della rete MTU
Attain DNS Automatically		Ottiene l'indirizzo del Server DNS automaticamente
DNS 1 (Primary DNS Server)		Verificare con quanto fornito dal vostro provider ISP
DNS 2 (Secondary DNS Server)		Verificare con quanto fornito dal vostro provider ISP
DNS 3 (Third DNS Server)		Verificare con quanto fornito dal vostro provider ISP

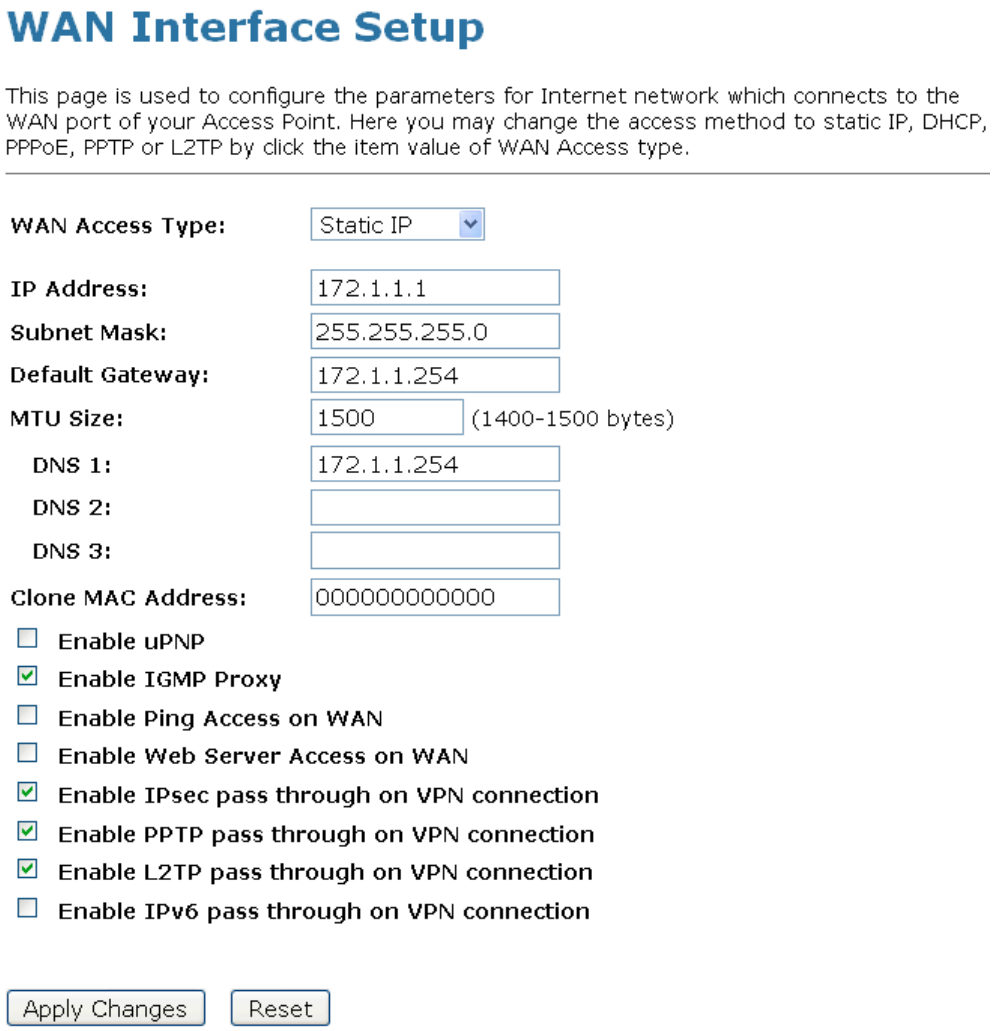
Opzione	Descrizione
Clone MAC Address	L'opzione di duplicazione dell'indirizzo MAC permette di identificare il dispositivo stesso come un computer o un dispositivo differente
Enable uPNP	Abilita o disabilita l' uPNP
Enable IGMP Proxy	Abilita o disabilita il Proxy IGMP
Enable Ping Access on WAN	Abilita o disabilita l'accesso alla funzione Ping su WAN
Enable Web Server Access on WAN	Abilita o disabilita il Web Server Access su WAN
Enable IPsec pass through on VPN connection	Abilita o disabilita la funzione “pass through” IPsec su connessione VPN
Enable PPTP pass through on VPN connection	Abilita o disabilita la funzione “pass through” PPTP pass through su connessione VPN
Enable L2TP pass through on VPN connection	Abilita o disabilita la funzione “pass through” L2TP su connessione VPN

Configurazione della connessione con IP statico

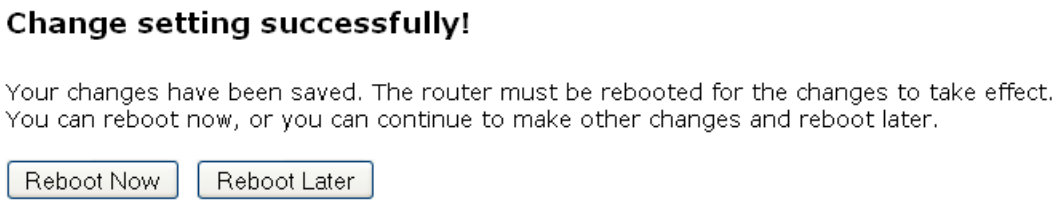
Se si dispone di una connessione con indirizzo IP fisso, digitare nei reltivi campi l'indirizzo IP, la Subnet Mask, l'indirizzo del Gateway e gli indirizzi di DNS (domain name server) forniti dal vostro ISP.

Se il contratto con l' ISP prevede una connessione con IP statico, attenersi alle seguenti istruzioni.

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*. Si visualizza la seguente pagina:
2. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *Static IP*.
3. Digitare nei seguenti campi della connessione WAN i valori forniti da Telecom o dal vostro Internet Service Provider (ISP): IP Address, Subnet Mask, Default Gateway e DNS.
4. Premere il pulsante *Apply Changes*.


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.
WAN Access Type:
Static IP
IP Address:
172.1.1.1
Subnet Mask:
255.255.255.0
Default Gateway:
172.1.1.254
MTU Size:
1500
(1400-1500 bytes)
DNS 1:
172.1.1.254
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Enable IPv6 pass through on VPN connection
Apply Changes
Reset

5. Si visualizza il seguente messaggio: *Le modifiche sono state correttamente effettuate!* Premere il pulsante *Reboot Now* per confermare.

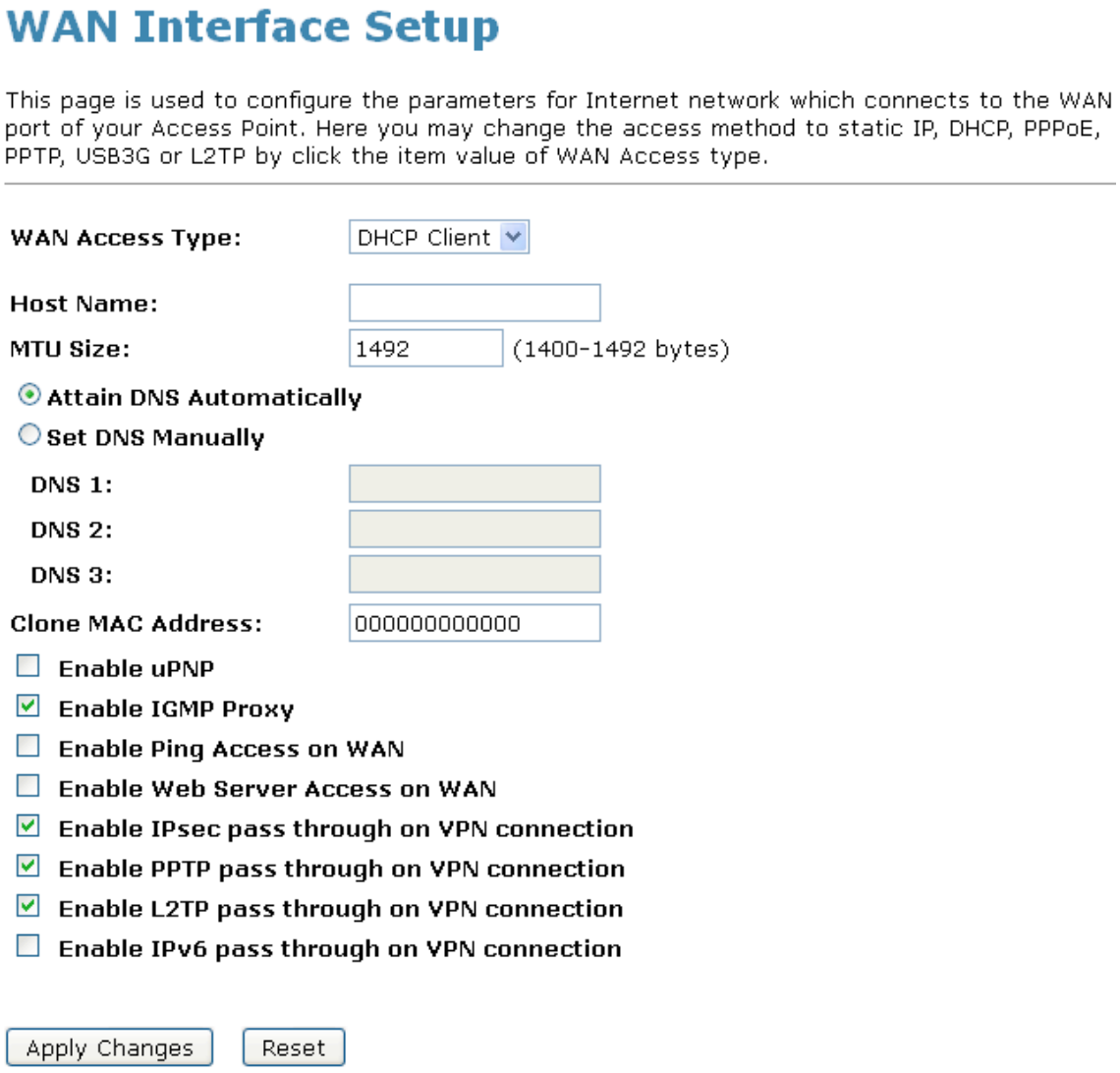

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

Configurazione della connessione DHCP Client

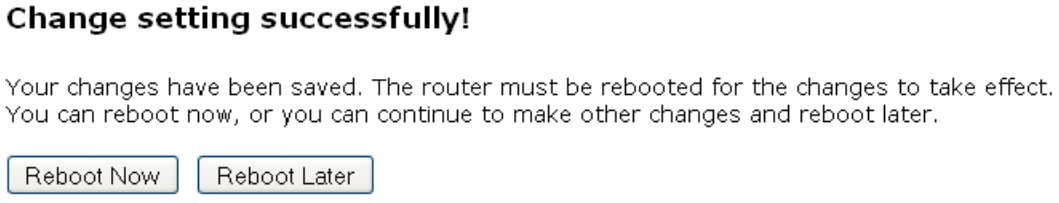
Dynamic Host Configuration Protocol (DHCP) con IP Dinamico (l'indirizzo IP lato WAN viene acquisito automaticamente). Se la connessione ad Internet si realizza mediante un Modem di linea, in questo caso l'indirizzo IP assegnato è di tipo dinamico.

Se il contratto con l'ISP prevede una connessione mediante DHCP Client, attenersi alle seguenti istruzioni.

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*. Si visualizza la seguente pagina:
2. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *DHCP Client*.
3. Premere il pulsante *Apply Changes*.


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Host Name:
MTU Size:
1492
(1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Enable IPv6 pass through on VPN connection
Apply Changes
Reset

4. Si visualizza il seguente messaggio: *Le modifiche sono state correttamente effettuate!* Premere il pulsante *Reboot Now* per confermare.

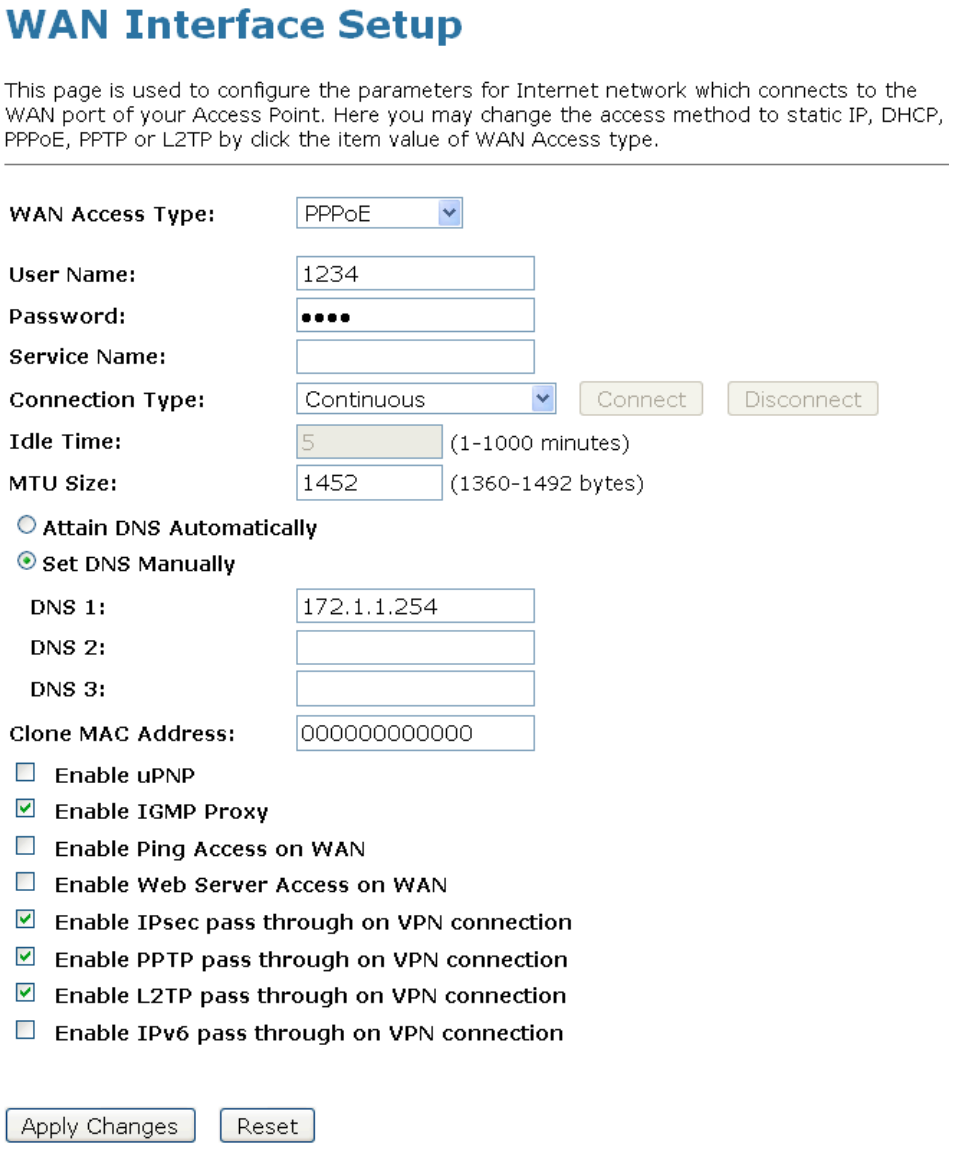

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

Configurazione della connessione mediante PPPoE

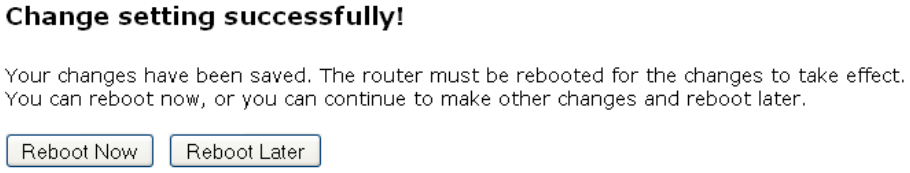
Se il vostro ISP prevede una connessione mediante PPPoE, è necessario configurare un account PPP. Al primo accesso ad Internet, l'ISP richiede di inserire Username e la Password fornita, così da verificare che la connessione viene effettuata da un utente registrato. Il dispositivo memorizza tali informazioni di autenticazione, così da non dover digitare Username e Password ad ogni accesso.

Se il contratto con l' ISP prevede una connessione mediante PPP, attenersi alle seguenti istruzioni.

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*.
2. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *PPPoE*.
3. Digitare lo *Username* e la *Password* forniti dall' ISP. Digitare ciascun valore nel relativo campo.
4. Premere il pulsante *Apply Changes*.



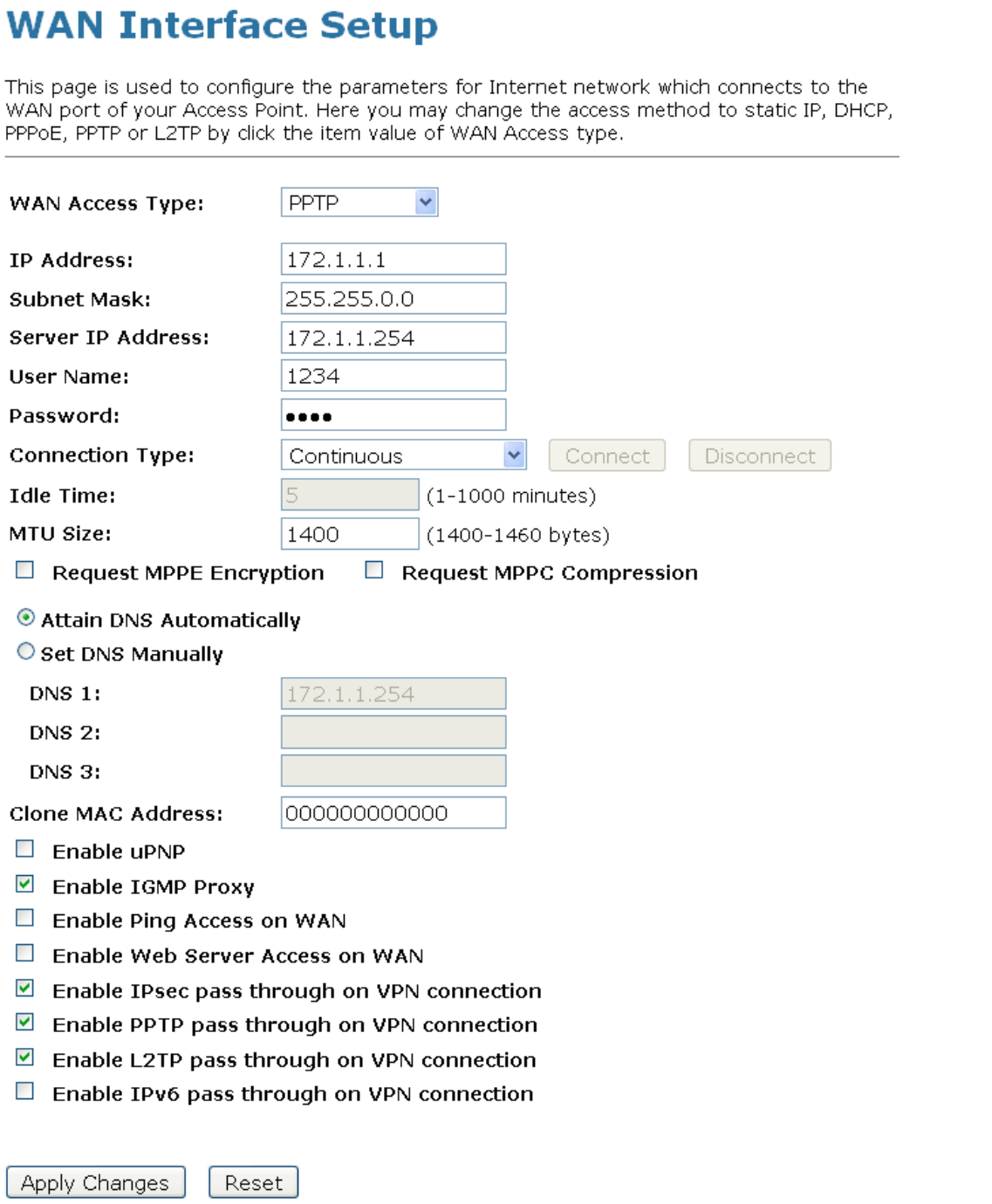
5. *Le modifiche sono state correttamente effettuate!* Premere *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

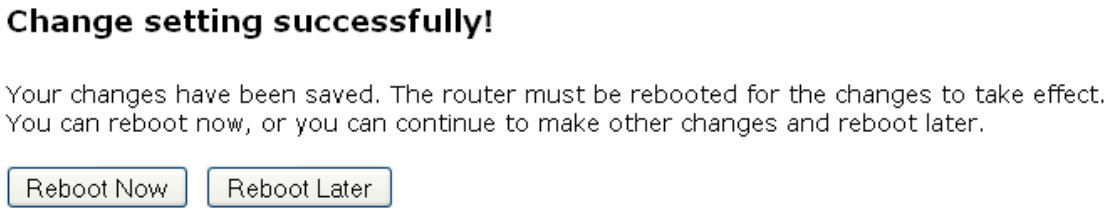
Configurazione della connessione mediante PPTP

Se il contratto con l' ISP o l'amministratore di rete prevede una connessione mediante PPTP, attenersi alle seguenti istruzioni.

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*. Si visualizza la seguente pagina:
2. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *PPTP*.
3. Digitare l'*indirizzo IP*, la *Subnet Mask*, l'*indirizzo IP del server*, lo *User Name* e la *Password* forniti dall' ISP. Digitare ciascun valore nel relativo campo.
4. Premere il pulsante *Apply Changes*.



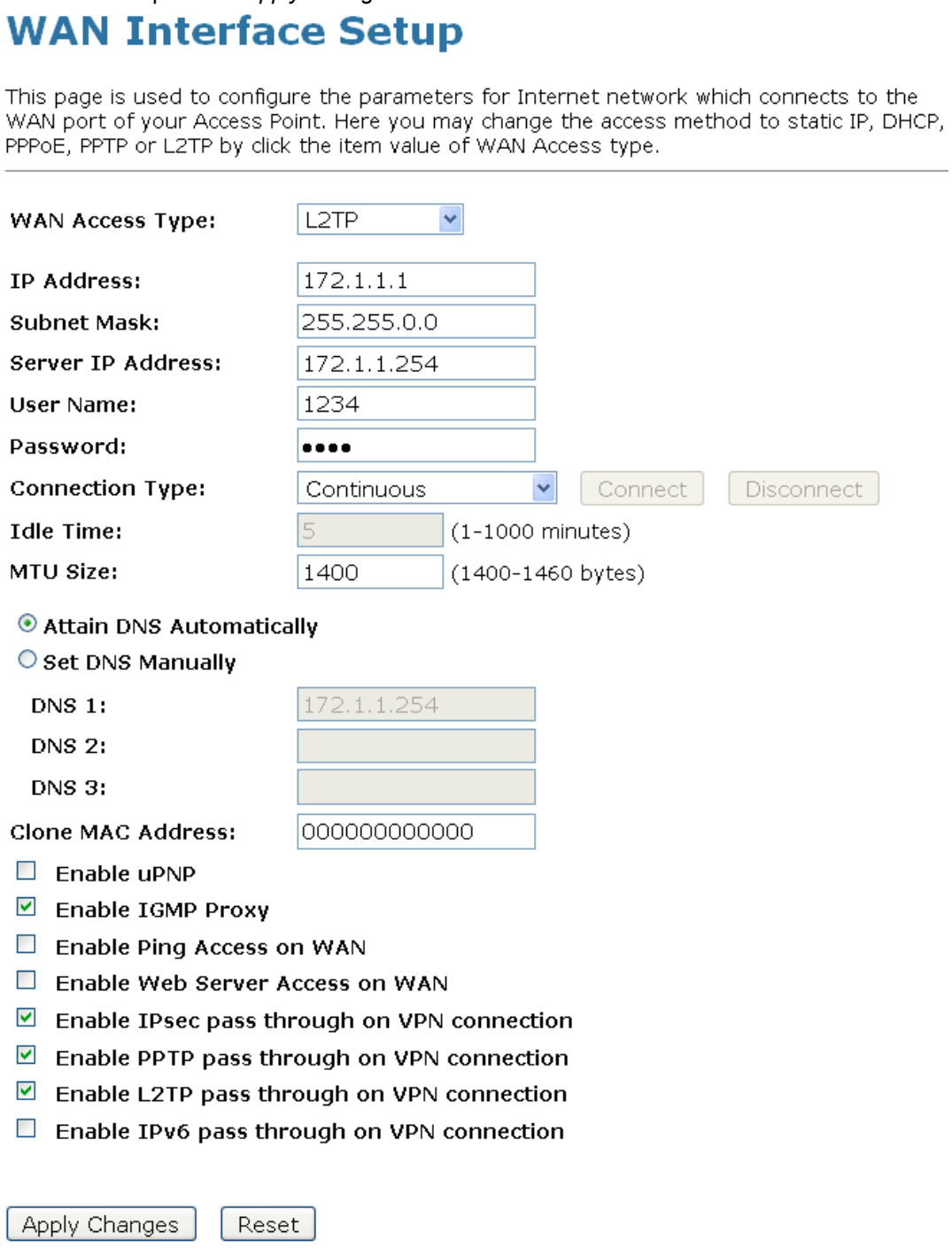
5. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

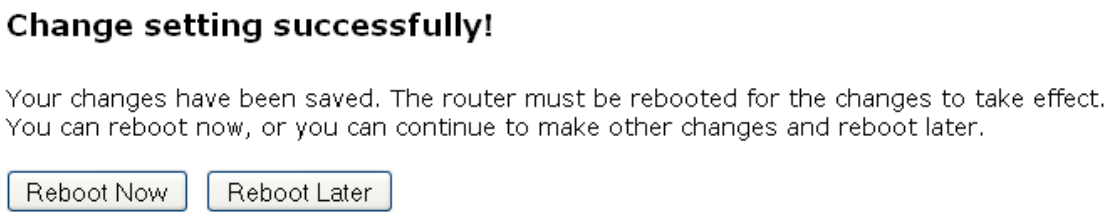
Configurazione della connessione mediante L2TP

Se il contratto con l' ISP o l'amministratore di rete prevede una connessione mediante L2TP, attenersi alle seguenti istruzioni.

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*. Si visualizza la seguente pagina:
2. Dall'elenco predefinito del campo *WAN Access Type*, selezionare *L2TP*.
3. Digitare l'*indirizzo IP*, la *Subnet Mask*, l'*indirizzo IP del server*, lo *User Name* e la *Password* forniti dall' ISP. Digitare ciascun valore nel relativo campo.
4. Premere il pulsante *Apply Changes*.



5. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

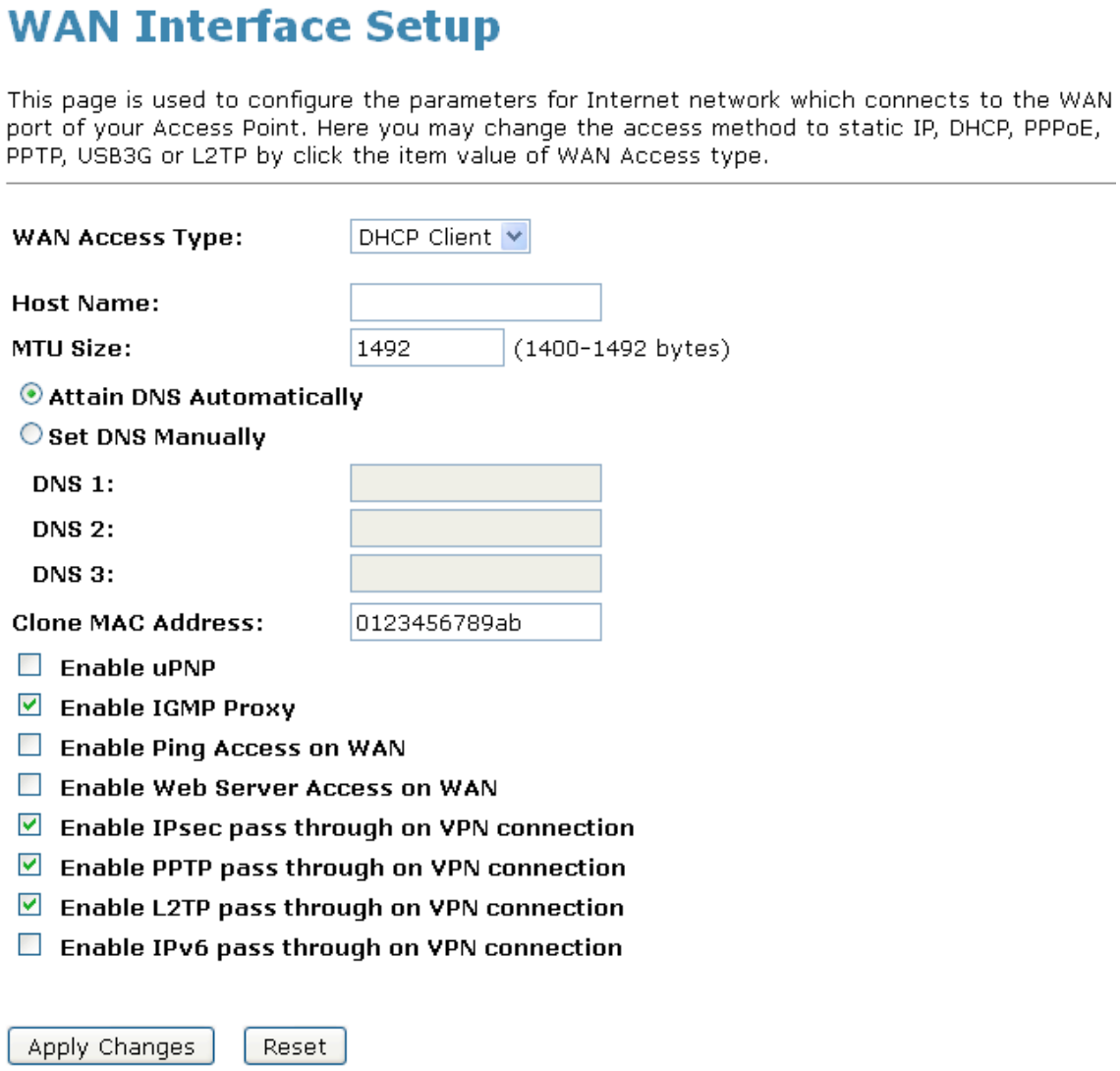

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

Duplicazione del MAC Address

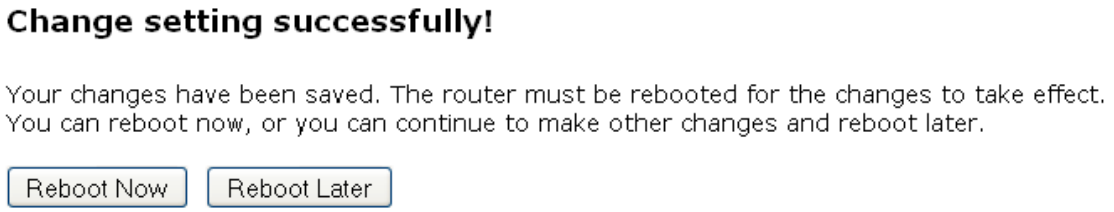
In alcuni casi particolari, l' ISP potrebbe richiedere che la connessione di casa e la connessione verso Internet mediante DSL/Modem di linea sia realizzata utilizzando lo stesso valore di MAC address, ossia quello della scheda di rete del computer. Qualora doveste cambiare la scheda di rete, sarà necessario contattare l'ISP per modificare il MAC address memorizzato. Il Router permette di modificare il proprio MAC address con lo stesso valore del computer che si è registrato originariamente con l'ISP.

La pagina seguente permette di abilitare o disabilitare tale funzione.

1. Dal menù di sinistra selezionare *Network Settings -> WAN Interface*. Si visualizza la seguente pagina:
2. Digitare il MAC address (per esempio 0123456789ab) che si vuole utilizzare in sostituzione del MAC address originario nel campo *Clone MAC Address*.
3. Se si digita 12 volte il valore 0 nel campo *Clone MAC Address*, tale funzione viene disabilitata.
4. Premere il pulsante *Apply Changes*.


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, USB3G or L2TP by click the item value of WAN Access type.
WAN Access Type:
DHCP Client
Host Name:
MTU Size:
1492
(1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
0123456789ab
Enable uPNP
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Enable IPsec pass through on VPN connection
Enable PPTP pass through on VPN connection
Enable L2TP pass through on VPN connection
Enable IPv6 pass through on VPN connection
Apply Changes
Reset

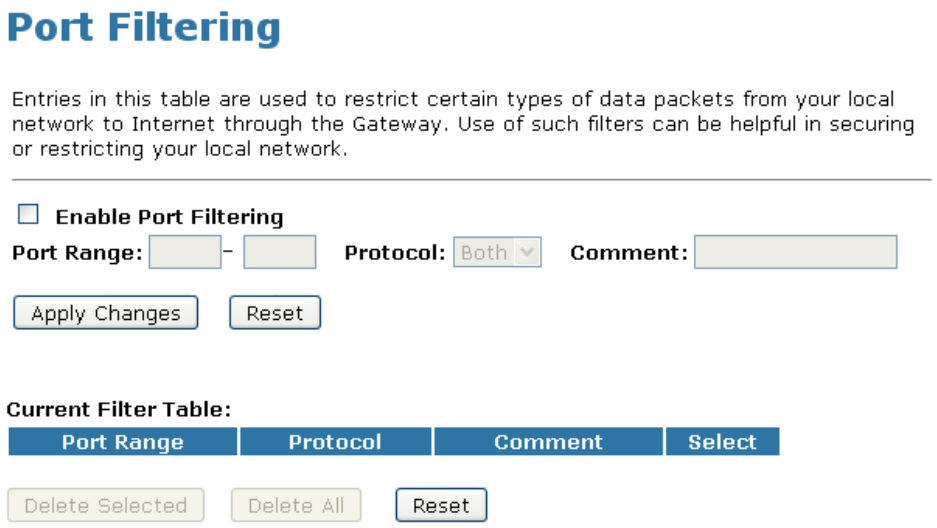
5. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

12 Filtri associati alle porte

I parametri registrati nella Tabella dei Filtri Attivi (*Current Filter Table*) sono utilizzati per limitare l'accesso di particolari porte e tipi di dati utilizzati nella rete locale, verso la rete esterna (Internet) attraverso il Router (Gateway). L'uso di specifici filtri può essere utilizzata per aumentare la sicurezza e ridurre l'accessibilità della rete locale.

1. Dal menù di sinistra, selezionare *Firewall -> Port Filtering*. Si visualizza la seguente pagina:


Port Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable Port Filtering
Port Range: - Protocol: Both Comment:
Apply Changes
Reset
Current Filter Table:
Port Range
Protocol
Comment
Select
Delete Selected
Delete All
Reset

Opzione	Descrizione
Enable Port Filtering	Abilita/disabilita i filtri sui pacchetti dati verso WAN. Di default è disabilitato.
Port Range	Range delle porte da filtrare per il flusso dati in ingresso ed in uscita
Protocol	Seleziona il protocollo da filtrare per il flusso dati in ingresso ed in uscita Both: Il filtro si applica sia per il protocollo TCP che UDP TCP: Il filtro si applica solo per il protocollo TCP UDP: Il filtro si applica solo per il protocollo UDP
Comment	Permette di inserire opportune note, così da consentire al manager di rete di conoscere le regole di filtratura applicate alle porte
Current Filter Table	Tale voce contiene l'elenco dei filtri creati ed applicati alle porte

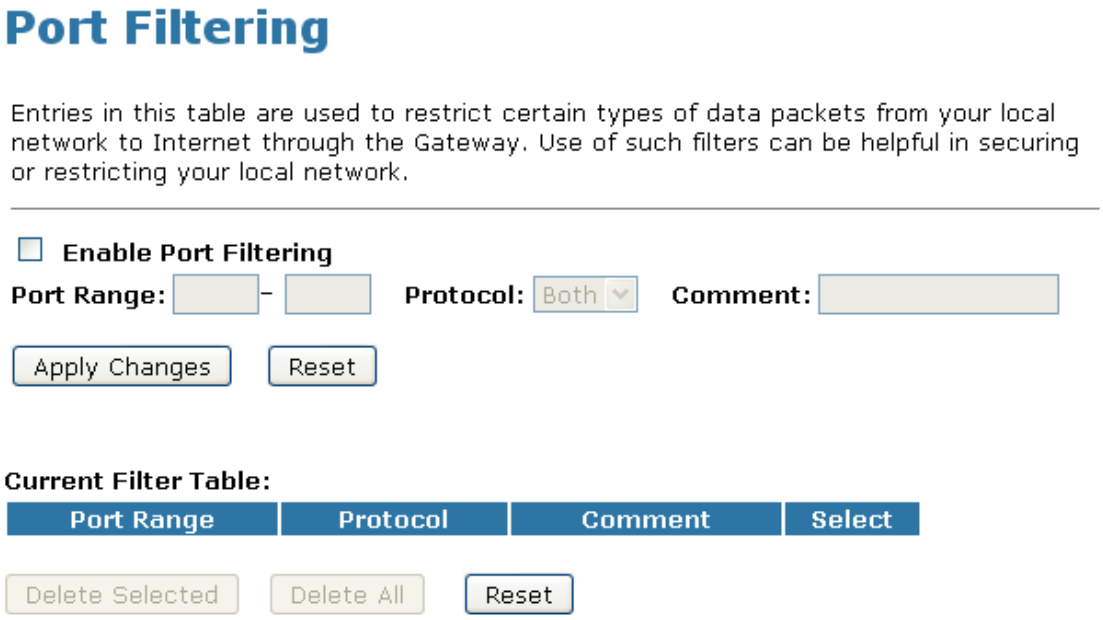
Nota

E' necessario assicurarsi che la singola porta o il range di porte su cui si applicano i filtri non siano utilizzati da applicazioni comuni o specifici in uso sulla rete. Verificare l'elenco delle porte comuni.

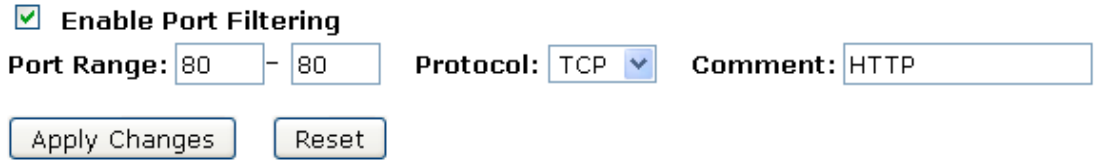
Filtro per la porta 80 - protocollo TCP

Si faccia riferimento all'esempio sottostante per bloccare il flusso dati in ingresso ed in uscita con protocollo TCP sulla porta 80.

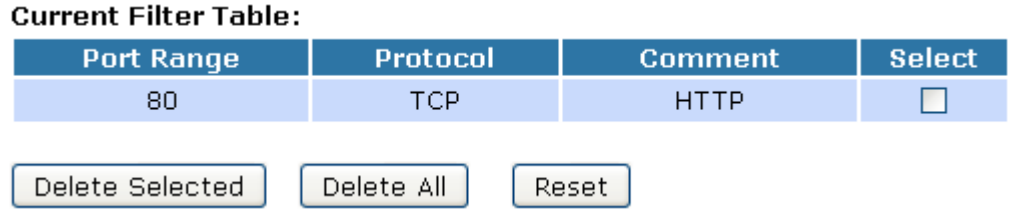
1. Dal menù di sinistra, selezionare *Firewall -> Port Filtering.* Si visualizza la seguente pagina:


Port Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable Port Filtering
Port Range: - Protocol: Both Comment:
Apply Changes
Reset
Current Filter Table:
Port Range
Protocol
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable Port Filtering* sia abilitata
3. Digitare 80 in entrambi i campi che definiscono il range di porte.
4. Selezionare dall'elenco del campo *Protocol* il valore *TCP*.
5. Digitare HTTP nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.



7. Il filtro creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo, il traffico dati di tipo TCP in ingresso ed in uscita dalla porta 80 viene bloccato.

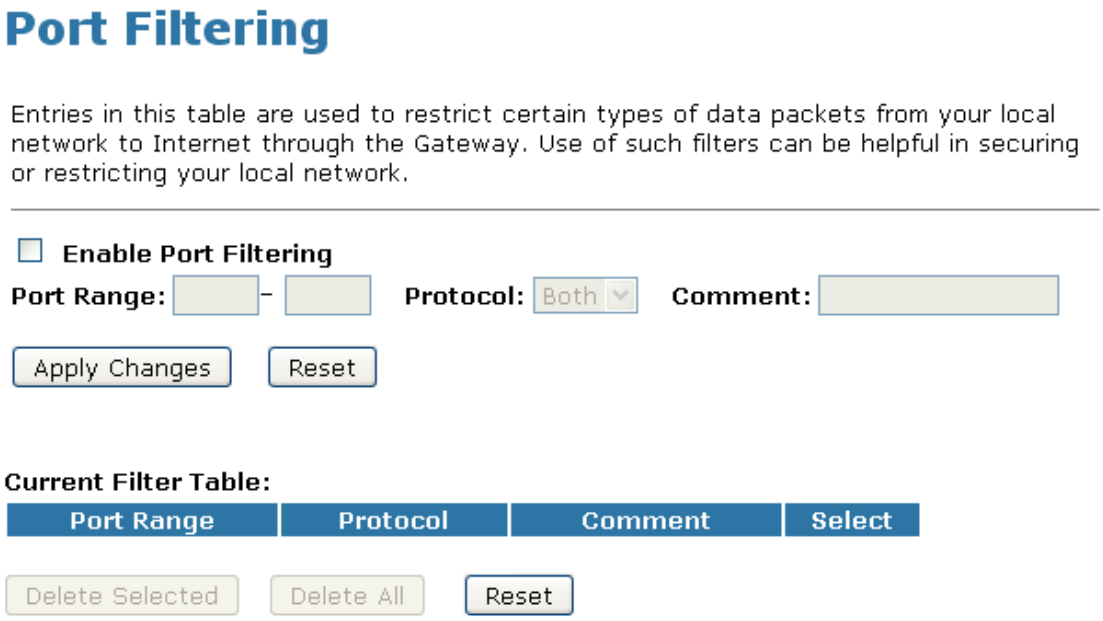


Così facendo non sarà più possibile visitare siti WEB, in quanto la porta 80 non permette il passaggio di dati con protocollo TCP, secondo le regole del filtro creato.

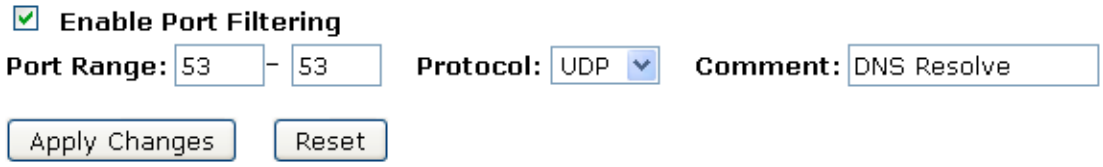
Filtro per la porta 53 protocollo UDP

Si faccia riferimento all'esempio sottostante per bloccare il flusso dati in ingresso ed in uscita con protocollo UDP sulla porta 53.

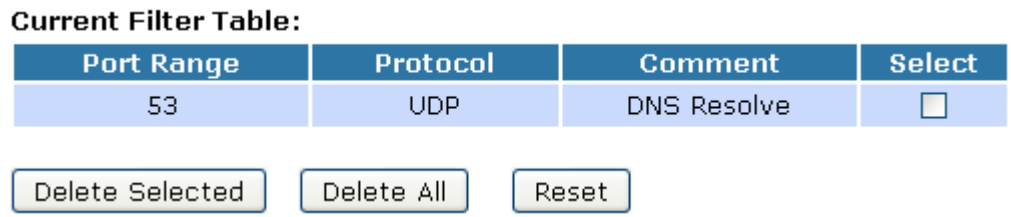
1. Dal menù di sinistra, selezionare *Firewall -> Port Filtering*. Si visualizza la seguente pagina:


Port Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable Port Filtering
Port Range: - Protocol: Both Comment:
Apply Changes
Reset
Current Filter Table:
Port Range
Protocol
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable Port Filtering* sia abilitata
3. Digitare 53 in entrambi i campi che definiscono il range di porte.
4. Selezionare dall'elenco del campo *Protocol* il valore *UDP*.
5. Digitare “Risoluzione DNS” nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.



7. Il filtro creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo, il traffico dati di tipo UDP in ingresso ed in uscita dalla porta 53 viene bloccato.



Così facendo non sarà più possibile visitare siti WEB per dominio, in quanto la porta 53 non permette il passagio di dati con protocollo UDP, secondo le regole del filtro creato.

E' ancora possibile visitare un sito WEB digitando il relativo indirizzo IP.

13 Filtri associati all'indirizzo IP

I parametri registrati in questa tabella sono utilizzati per limitare l'accesso di particolari tipi di dati dalla rete locale verso la rete esterna (Internet) attraverso il Router (Gateway). L'uso di specifici filtri può essere utile per aumentare la sicurezza e ridurre l'accessibilità della rete locale.

La funzione Filtri IP permette di impostare delle regole per il controllo dei flussi dati entranti ed uscenti tra la LAN e la WAN.

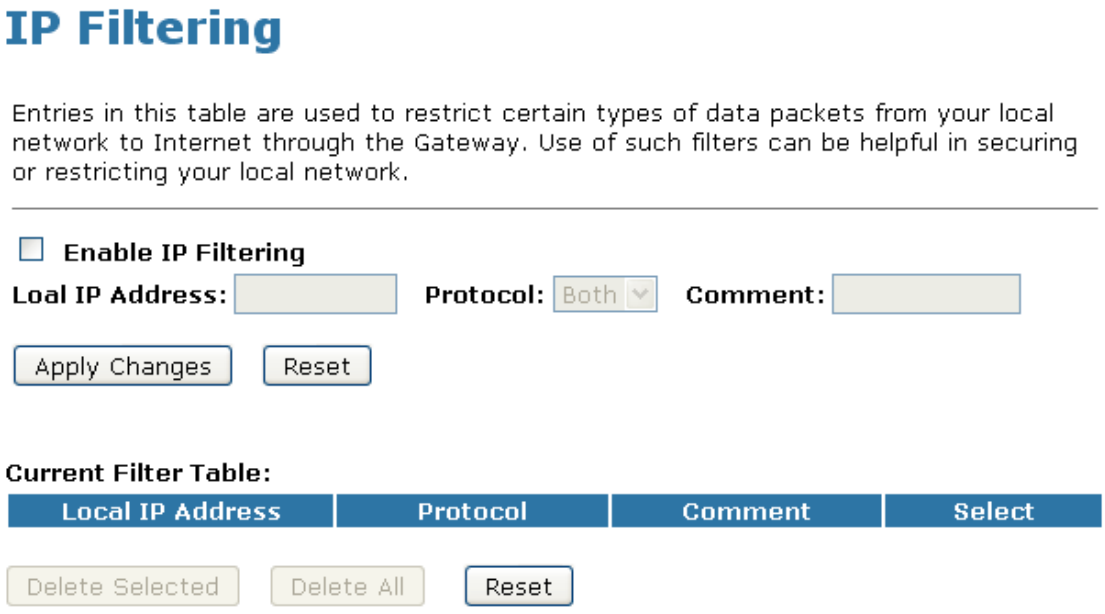
E' possibile creare filtri per bloccare l'accesso da specifici computer della rete locale LAN verso specifici siti Internet e tipi di dati. Analogamente è possibile bloccare l'accesso dalla WAN ai computer in rete LAN.

Quando si definisce una regola per applicare un filtro IP e si abilita tale filtro, il router ADSL/Ethernet esaminerà i pacchetti dati in transito per determinare se soddisfano o meno la regola imposta dal filtro. Il filtro può applicarsi per il protocollo di rete o Internet, il pacchetto dati trasportato, la direzione del pacchetto dati (ad esempio, dalla LAN verso la WAN e viceversa).

Se il pacchetto dati soddisfa la regola imposta dal filtro, questo può essere accettato (e quindi reindirizzato al destinatario) oppure respinto (eliminato), in funzione della specifica azione del filtro.

La schermata IP Filter Configuration permette di abilitare/disabilitare la funzione di filtri IP ed i singoli filtri IP inseriti.

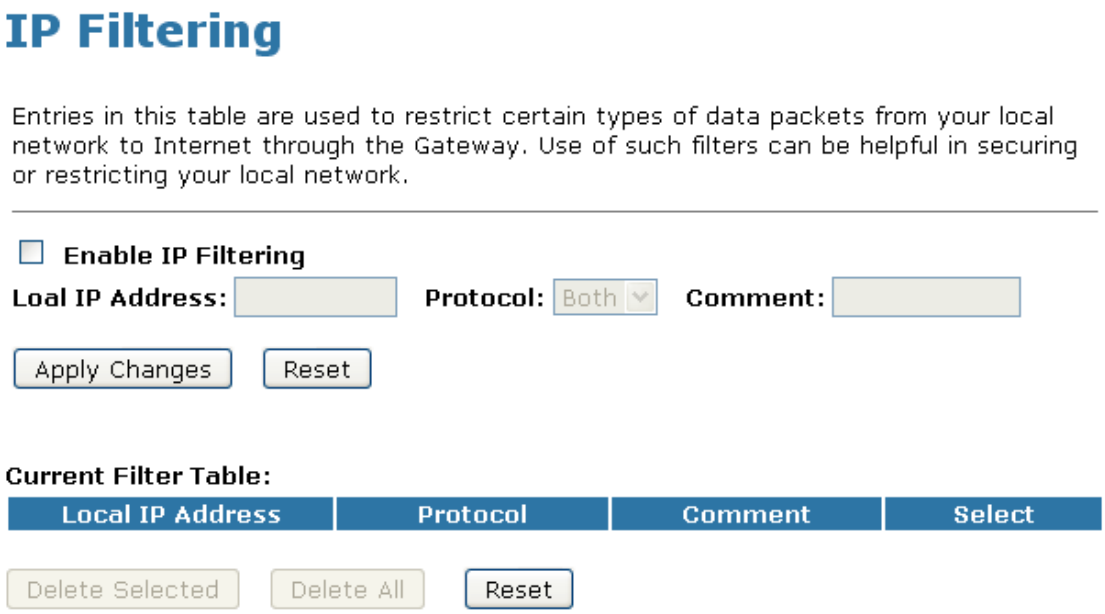
1. Dal menù di sinistra, selezionare *Firewall -> IP Filtering*. Si visualizza la seguente pagina:



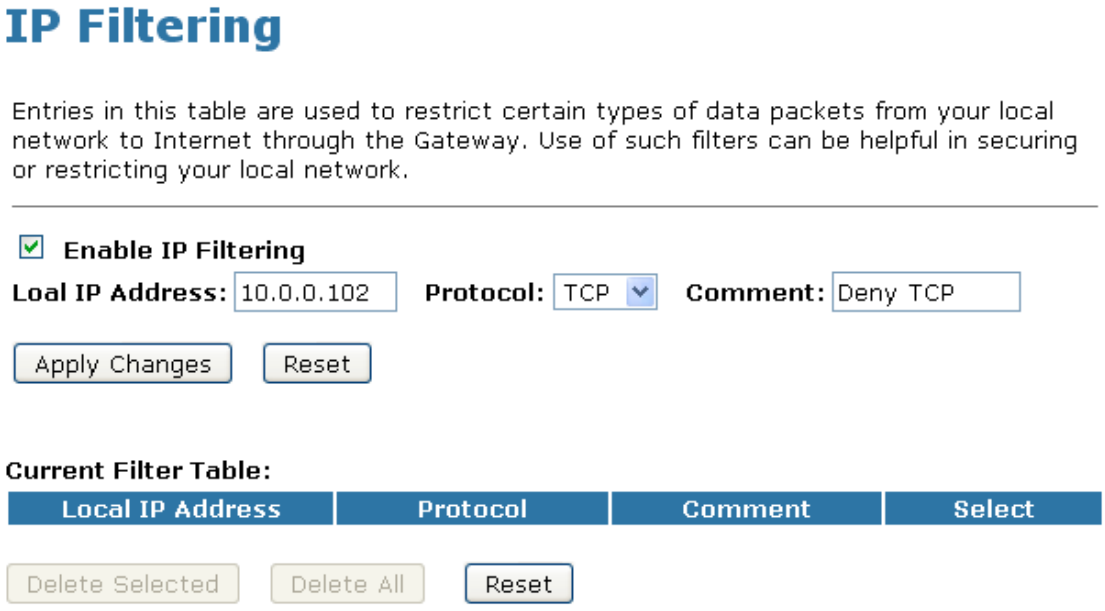
Filtri IP per protocollo TCP con indirizzo IP specifico

Si faccia riferimento all'esempio sottostante per bloccare il flusso dati in ingresso ed in uscita con protocollo TCP per uno specifico indirizzo IP.

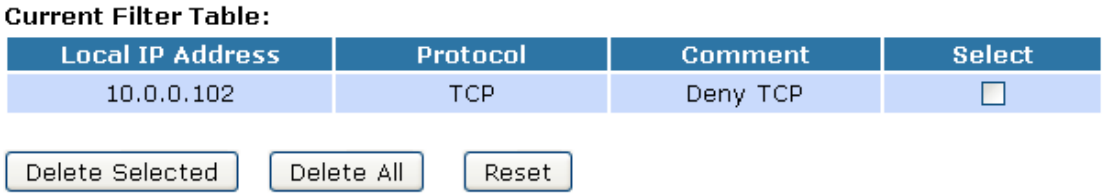
1. Dal menù di sinistra, selezionare *Firewall -> IP Filtering*. Si visualizza la seguente pagina:


IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address:
Protocol: Both
Comment:
Apply Changes
Reset
Current Filter Table:
Local IP Address
Protocol
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable IP Filtering* sia abilitata.
3. Digitare l'indirizzo IP che si vuole bloccare nel campo *Local IP Address*.
4. Selezionare dall'elenco del campo *Protocol* il valore *TCP*.
5. Digitare una descrizione esplicativa nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.


IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address: 10.0.0.102
Protocol: TCP
Comment: Deny TCP
Apply Changes
Reset
Current Filter Table:
Local IP Address
Protocol
Comment
Select
Delete Selected
Delete All
Reset

7. Il filtro IP creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo, il traffico dati di tipo TCP in ingresso ed in uscita viene bloccato.

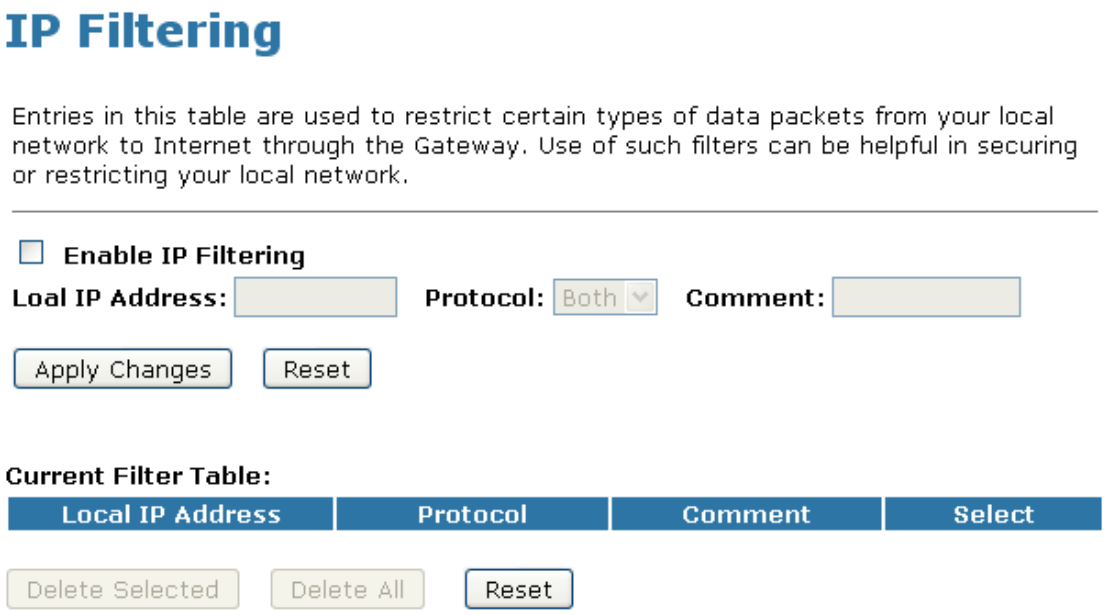


L'indirizzo IP locale (ad esempio il 10.0.0.102) elencato nella *Current Filter Table* non potrà più utilizzare alcuna applicazione che utilizzi il protocollo TCP, ad esempio per accedere a siti WEB.

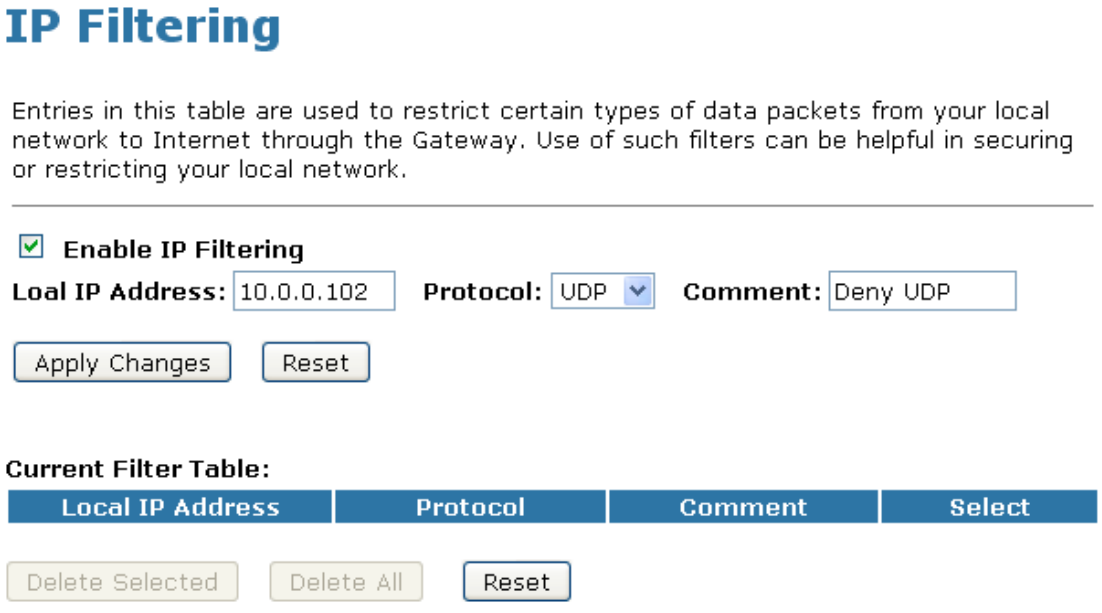
Filtri IP per protocollo UDP con indirizzo IP

Si faccia riferimento all'esempio sottostante per bloccare il flusso dati in ingresso ed in uscita con protocollo UDP per uno specifico indirizzo IP.

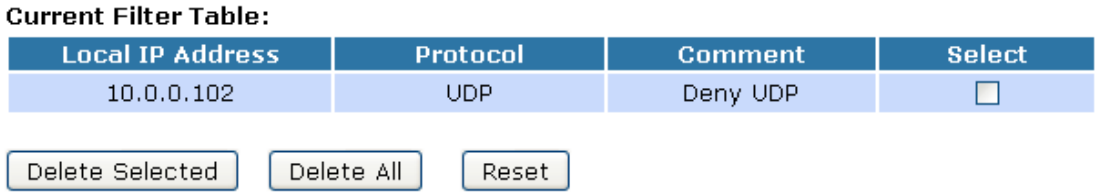
1. Dal menù di sinistra, selezionare *Firewall -> IP Filtering*. Si visualizza la seguente pagina:


IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address:
Protocol: Both
Comment:
Apply Changes
Reset
Current Filter Table:
Local IP Address
Protocol
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable IP Filtering* sia abilitata.
3. Digitare l'indirizzo IP che si vuole bloccarenel campo *Local IP Address*.
4. Selezionare dall'elenco del campo *Protocol* il valore *UDP*.
5. Digitare una descrizione esplicativa nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.


IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address: 10.0.0.102
Protocol: UDP
Comment: Deny UDP
Apply Changes
Reset
Current Filter Table:
Local IP Address
Protocol
Comment
Select
Delete Selected
Delete All
Reset

7. Il filtro IP creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo, il traffico dati di tipo UDP in ingresso ed in uscita viene bloccato.

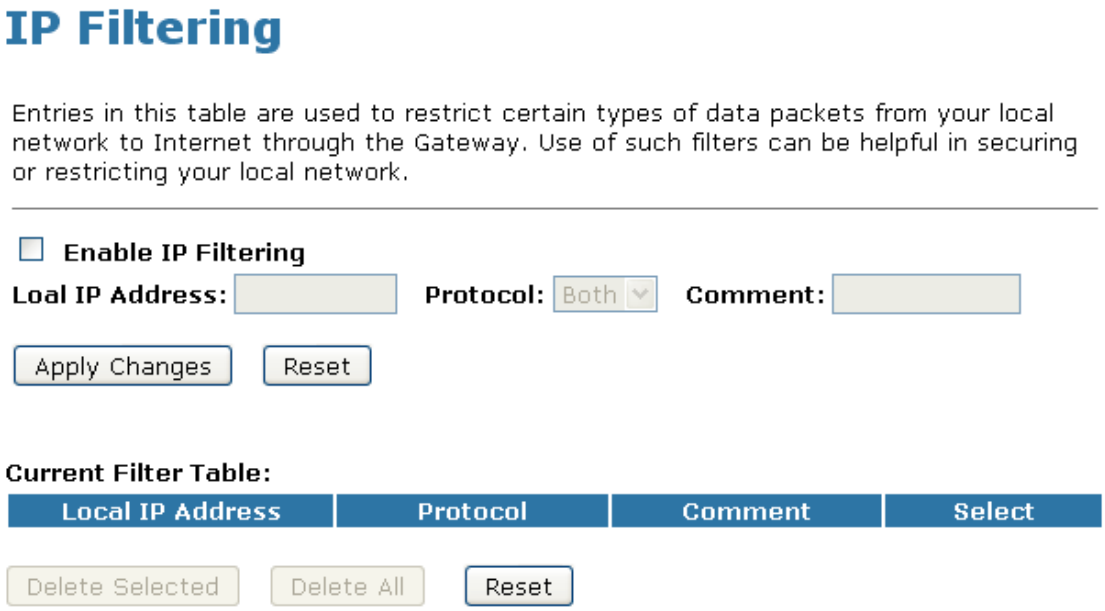


L'indirizzo IP locale (ad esempio il 10.0.0.102) elencato nella *Current Filter Table* non potrà più utilizzare alcuna applicazione che utilizzi il protocollo UDP, ad esempio il servizio TFTP.

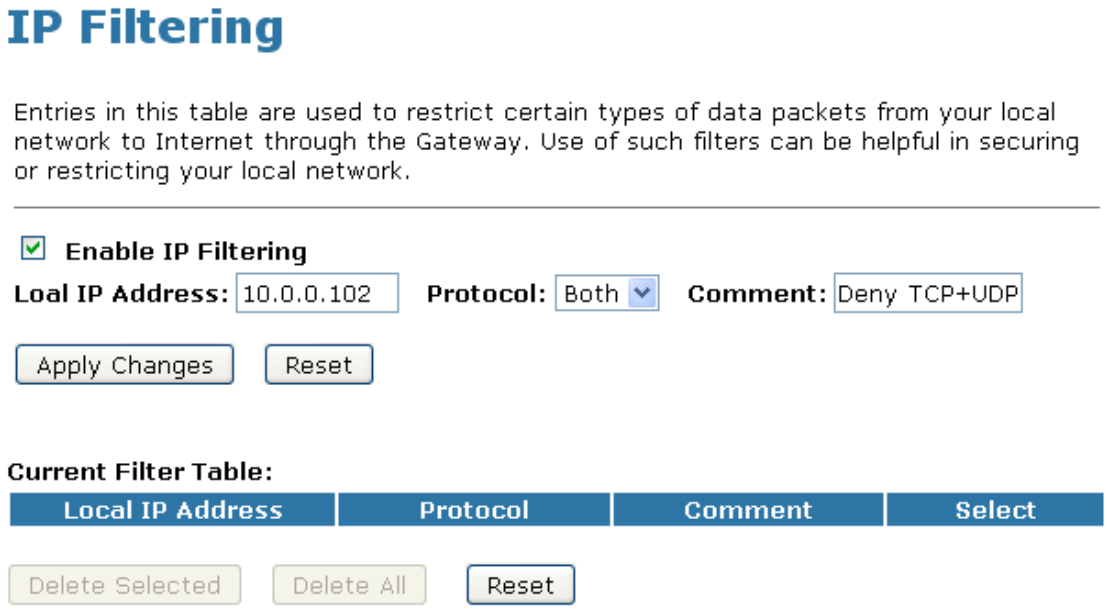
Filtri IP per entrambi i protocolli TCP e UDP con indirizzo IP specifico

Si faccia riferimento all'esempio sottostante per bloccare il flusso dati in ingresso ed in uscita con entrambi i protocolli TCP e UDP per uno specifico indirizzo IP.

1. Dal menù di sinistra, selezionare *Firewall -> IP Filtering*. Si visualizza la seguente pagina:


IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address:
Protocol: Both
Comment:
Apply Changes
Reset
Current Filter Table:
Local IP Address
Protocol
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable IP Filtering* sia abilitata.
3. Digitare l'indirizzo IP che si vuole bloccare nel campo *Local IP Address*.
4. Selezionare dall'elenco del campo *Protocol* il valore *Both*.
5. Digitare una descrizione esplicativa nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.


IP Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable IP Filtering
Loal IP Address: 10.0.0.102
Protocol: Both
Comment: Deny TCP+UDP
Apply Changes
Reset
Current Filter Table:
Local IP Address
Protocol
Comment
Select
Delete Selected
Delete All
Reset

7. Il filtro IP creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo, il traffico dati di tipo sia TCP che UDP in ingresso ed in uscita viene bloccato.

Current Filter Table:

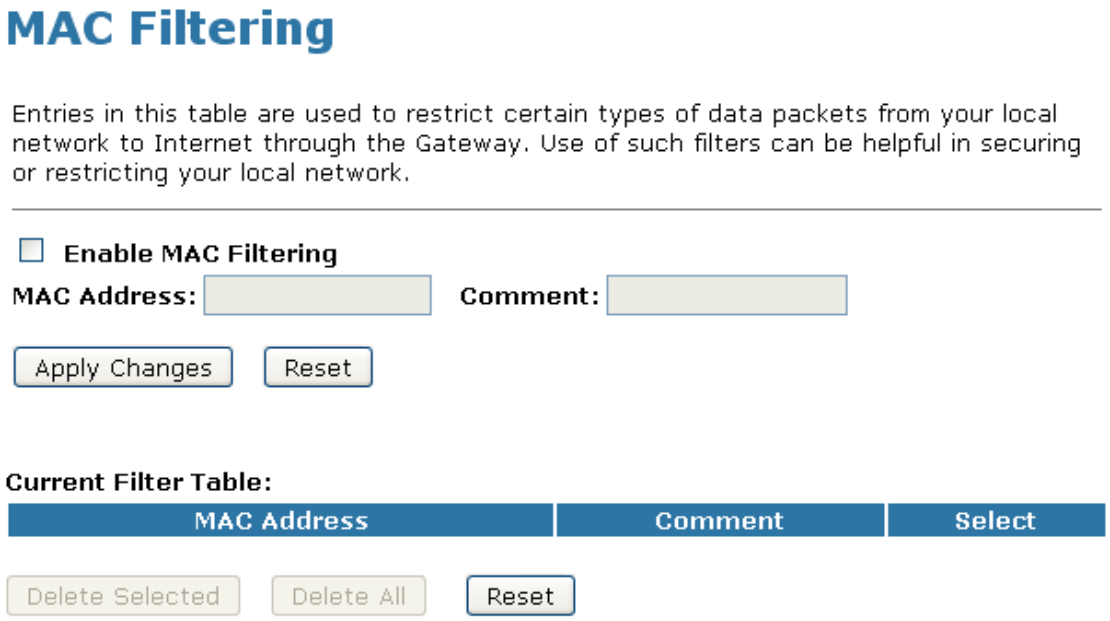
Local IP Address	Protocol	Comment	Select
10.0.0.102	TCP+UDP	Deny TCP+UDP	☐

Delete Selected Delete All Reset

14 Filtri associate al MAC Address

I paramateri registrati in questa tabella sono utilizzati per limitare l'accesso di particolari tipi di dati dalla rete locale verso la rete esterna (Internet) attraverso il Router (Gateway). L'uso di specifici filtri può essere utilizzata per aumentare la sicurezza e ridurre l'accessibilità della rete locale.

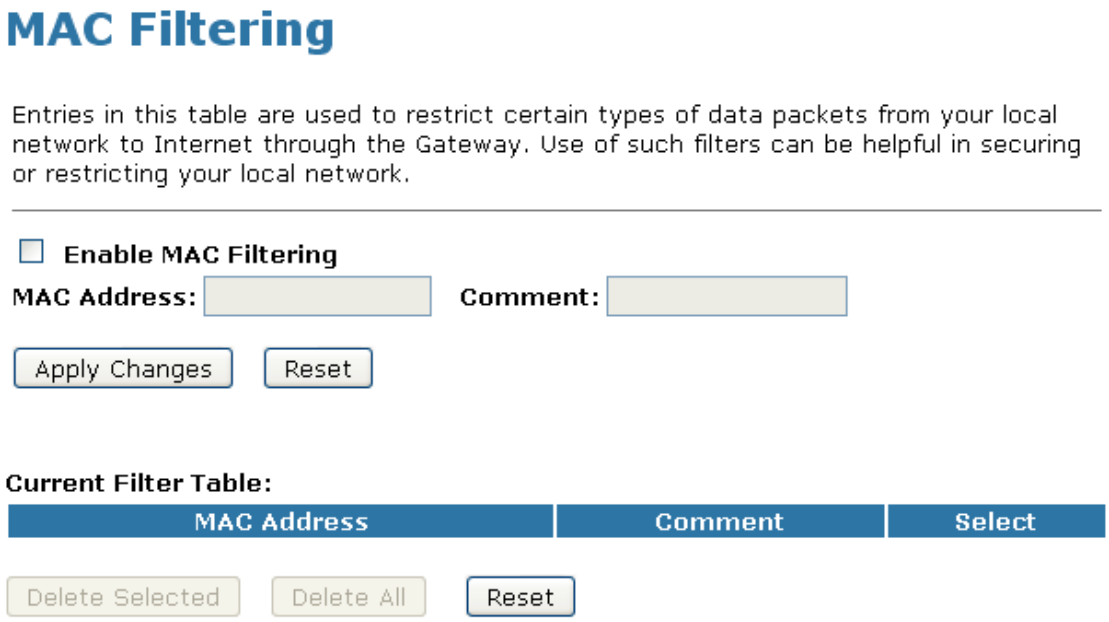
1. Dal menù di sinistra, selezionare *Firewall -> MAC Filtering*. Si visualizza la seguente pagina:


MAC Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable MAC Filtering
MAC Address:
Comment:
Apply Changes
Reset
Current Filter Table:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Filtri associate a specifici MAC Address

Si faccia riferimento all'esempio sottostante per bloccare l'accesso ad Internet a specifici MAC address.

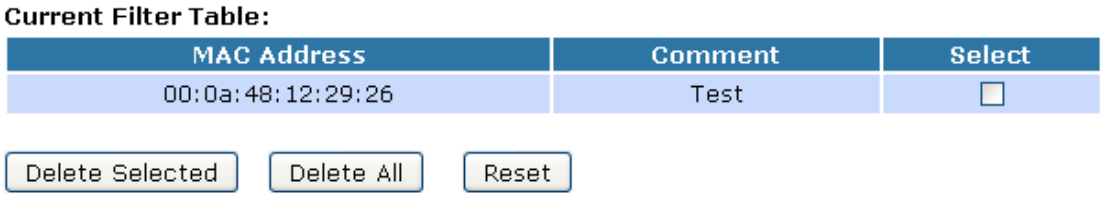
1. Dal menù di sinistra, selezionare *Firewall -> MAC Filtering*. Si visualizza la seguente pagina:


MAC Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable MAC Filtering
MAC Address:
Comment:
Apply Changes
Reset
Current Filter Table:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable MAC Filtering* sia abilitata.
3. Digitare il MAC Address a cui si vuole bloccare l'accesso nel campo *MAC Address*.
4. Digitare una descrizione esplicativa nel campo *Comment*.
5. Premere il pulsante *Apply Changes*.

MAC Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable MAC Filtering
MAC Address: 000a48122926
Comment: Test
Apply Changes
Reset
Current Filter Table:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

6. Il filtro creato viene automaticamente aggiunto alla *Current Filter Table*.
7. In tal modo il MAC Address relativo al filtro creato non avrà più accesso ad Internet.



15 Reindirizzamento porte

I valori della tabella di reindirizzamento porte permettono di reindirizzare automaticamente servizi comuni di rete a macchine specifiche tramite il firewall NAT. Tali configurazioni sono necessarie solo se si vuole ospitare server particolari, quali Web Server o server di posta sulla propria rete locale, utilizzando il firewall NAT del Router.

Il dispositivo è dotato di funzionalità specifiche in grado di garantire la sicurezza della rete locale, bloccando il traffico indesiderato da Internet.

Tali funzionalità non devono essere utilizzate se si vuole utilizzare il Router per una semplice connessione ad Internet dalla propria rete locale. In questo caso non sono richieste modifiche alla configurazione di default delle funzionalità di Sicurezza del Router. E' necessario apportare modifiche alla configurazione solamente a fronte di uno o ad entrambi i seguenti casi:

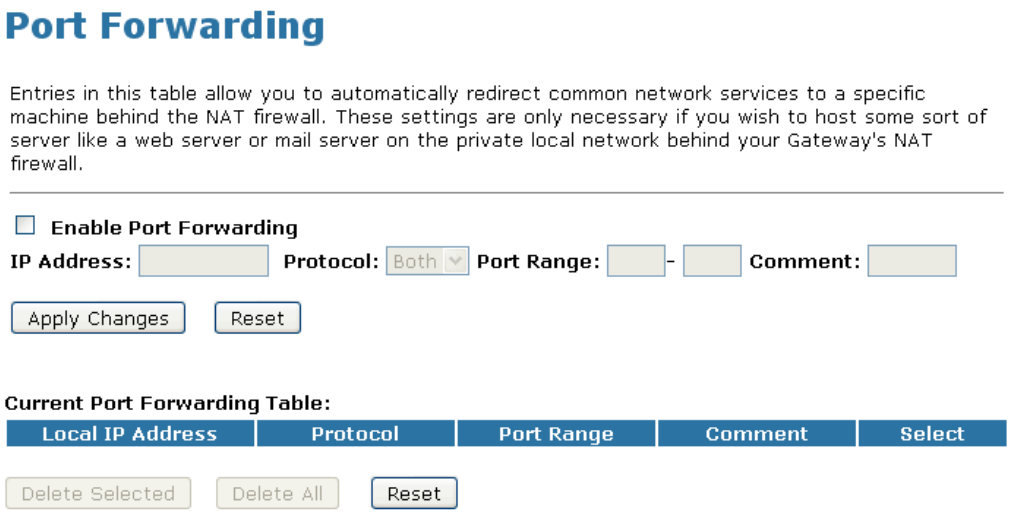
- permettere ad utenti di internet di accedere a pagine WEB localizzate su macchine in rete locale (ad esempio, per realizzare un server FTP o HTTP)
- utilizzare particolari giochi che richiedono l'accessibilità del computer locale da Internet

Il capitolo descrive come configurare la Sicurezza per adeguarsi alle necessità della rete.

Di default, gli indirizzi IP in uso sulla rete locale sono nascosti dal lato di Internet. Tutti i dati trasmessi dai PC della rete locale ad un PC su Internet sono identificati mediante l'indirizzo IP esterno del Router.

In questo modo i dettagli relativi alla rete locale LAN rimangono privati. Questa caratteristica di sicurezza è denominata "*Port Forwarding*" (reindirizzamento porte).

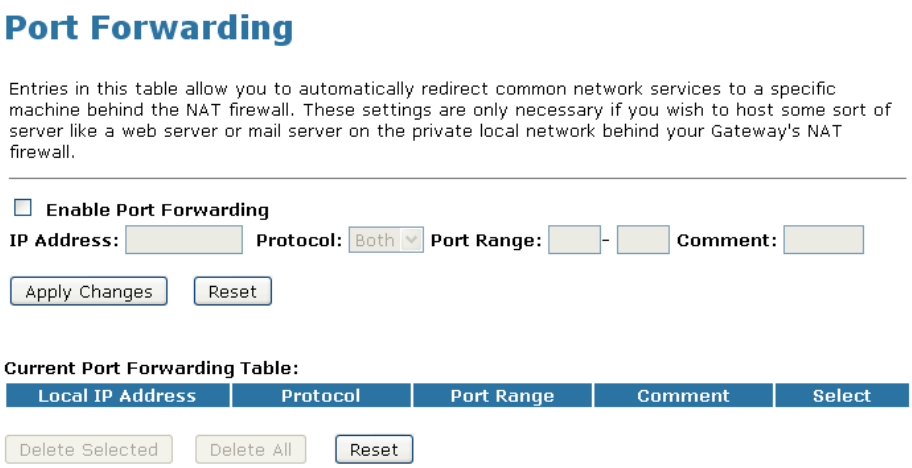
1. Dal menù di sinistra, selezionare *Firewall -> Port Forwarding*. Si visualizza la seguente pagina:


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address:
Protocol: Both
Port Range: -
Comment:
Apply Changes
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Port Range
Comment
Select
Delete Selected
Delete All
Reset

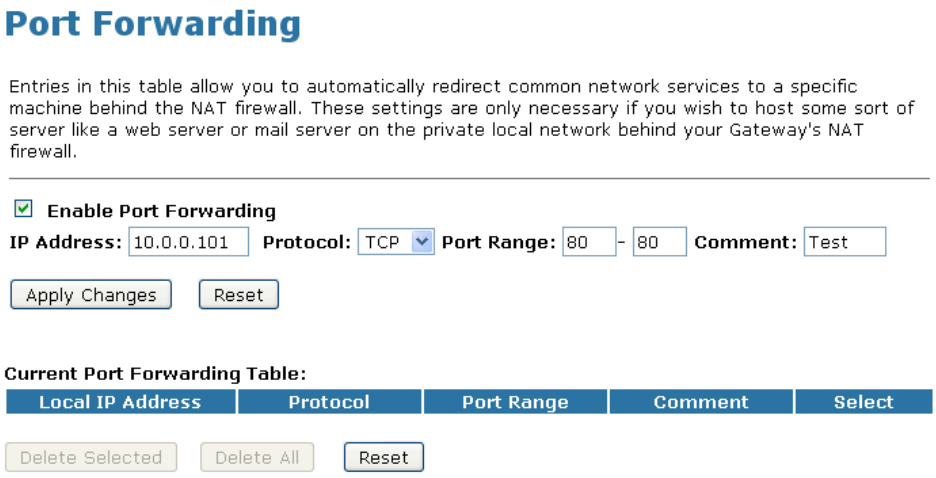
Reindirizzamento porte per protocollo TCP con specifico indirizzo IP

Si faccia riferimento all'esempio sottostante per configurare il reindirizzamento delle porte con protocollo TCP per uno specifico indirizzo IP.

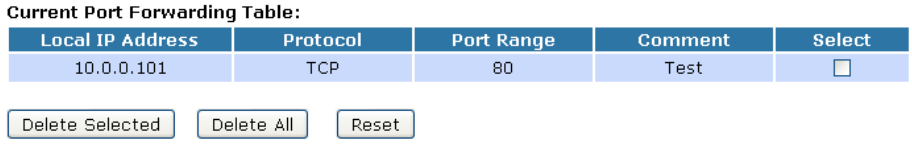
1. Dal menù di sinistra, selezionare *Firewall -> Port Forwarding*. Si visualizza la seguente pagina:


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address:
Protocol: Both
Port Range:
Comment:
Apply Changes
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Port Range
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable Port Forwarding* sia abilitata.
3. Digitare l'indirizzo IP a cui si vuole reindirizzare la porta nel campo *IP Address*.
4. Selezionare dall'elenco del campo *Protocol* il valore *TCP*.
5. Digitare una descrizione esplicativa nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address: 10.0.0.101
Protocol: TCP
Port Range: 80 - 80
Comment: Test
Apply Changes
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Port Range
Comment
Select
Delete Selected
Delete All
Reset

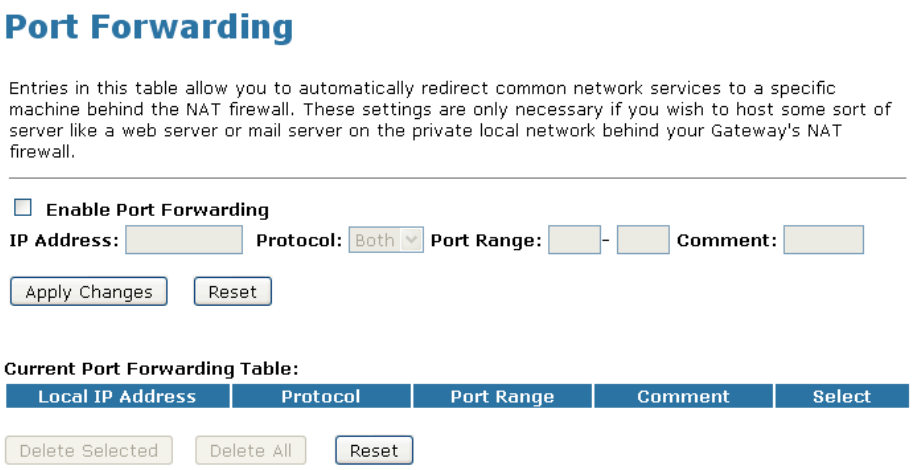
7. L'indirizzo IP ed il range di porte da reindirizzare che si è creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo il range di porte dell'indirizzo IP inserito nella *Current Filter Table* è reso accessibile da Internet mediante protocollo TCP.



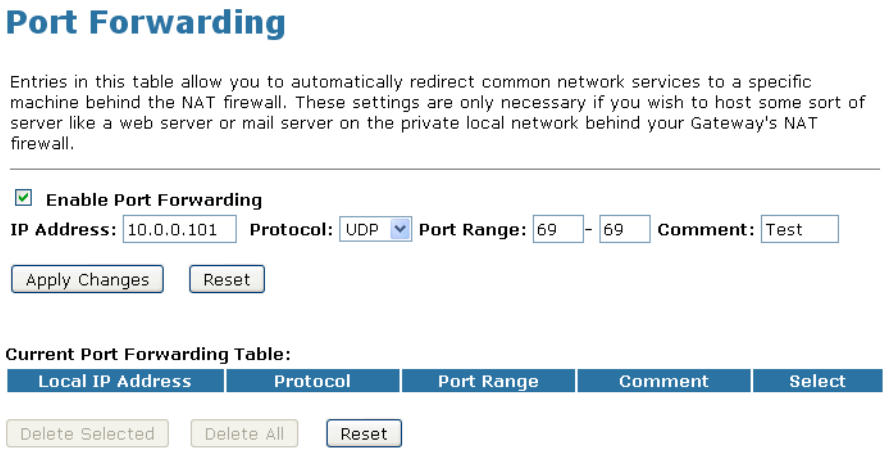
Reindirizzamento porte per protocollo UDP con specifico indirizzo IP

Si faccia riferimento all'esempio sottostante per configurare il reindirizzamento delle porte con protocollo UDP per uno specifico indirizzo IP.

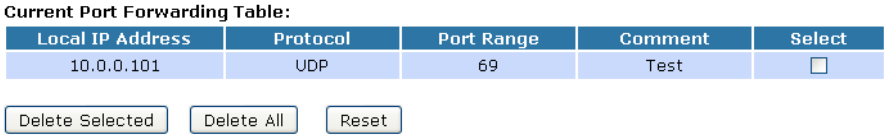
1. Dal menù di sinistra, selezionare *Firewall -> Port Forwarding*. Si visualizza la seguente pagina:


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address:
Protocol: Both
Port Range:
Comment:
Apply Changes
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Port Range
Comment
Select
Delete Selected
Delete All
Reset

2. Verificare che l'opzione *Enable Port Forwarding* sia abilitata.
3. Digitare l'indirizzo IP a cui si vuole reindirizzare la porta nel campo *IP Address*.
4. Selezionare dall'elenco del campo *Protocol* il valore *UDP*.
5. Digitare una descrizione esplicativa nel campo *Comment*.
6. Premere il pulsante *Apply Changes*.


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
IP Address: 10.0.0.101
Protocol: UDP
Port Range: 69 - 69
Comment: Test
Apply Changes
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Port Range
Comment
Select
Delete Selected
Delete All
Reset

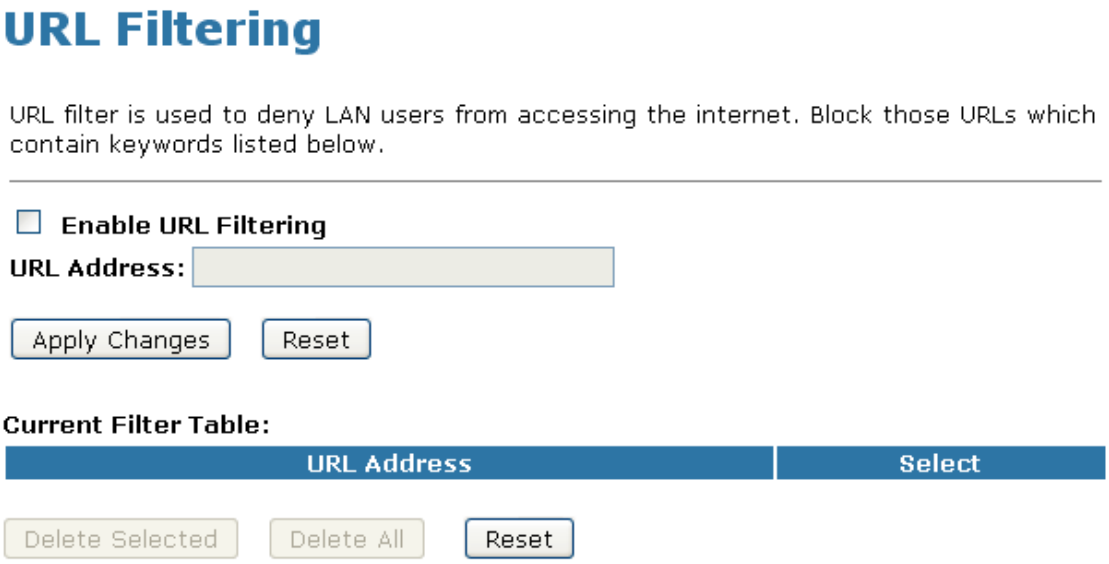
7. L'indirizzo IP ed il range di porte da reindirizzare che si è creato viene automaticamente aggiunto alla *Current Filter Table*.
8. In tal modo il range di porte dell'indirizzo IP inserito nella Current Filter Table è reso accessibile da Internet mediante protocollo UDP.



16 Filtri associati all'indirizzo URL

Il filtro associato all'URL si utilizza per bloccare l'accesso ad Internet agli utenti della LAN. Il filtro blocca l'accesso agli URL che contengono le parole chiave elencate di seguito.

1. Dal menù di sinistra, selezionare *Firewall -> URL Filtering*. Si visualizza la seguente pagina:



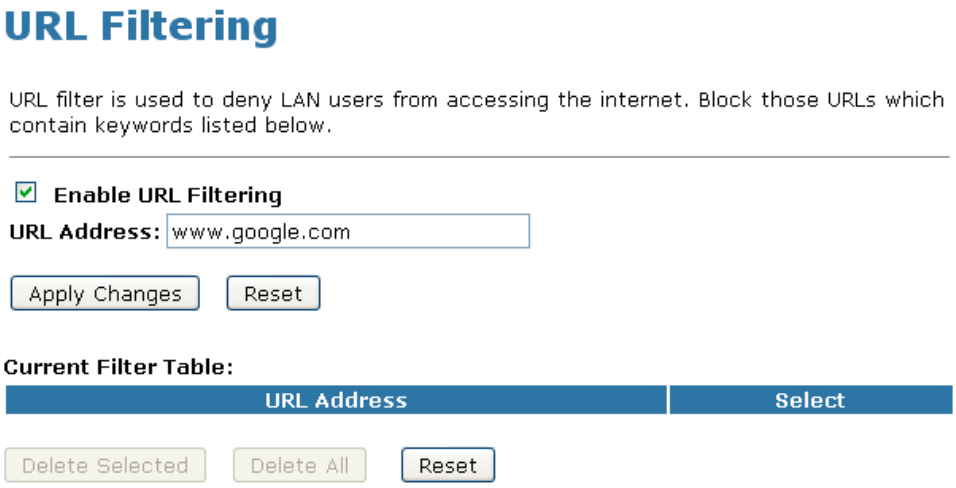
Filtri associati a specifici URL

Si faccia riferimento all'esempio sottostante per bloccare l'accesso ad Internet agli utenti della rete LAN.

1. Dal menù di sinistra, selezionare *Firewall -> URL Filtering*. Si visualizza la seguente pagina:

2. Verificare che l'opzione *Enable URL Filtering* sia abilitata.
3. Digitare l'URL (indirizzo del sito) che si vuole bloccare agli utenti della LAN.

4. Premere il pulsante *Apply Changes*.

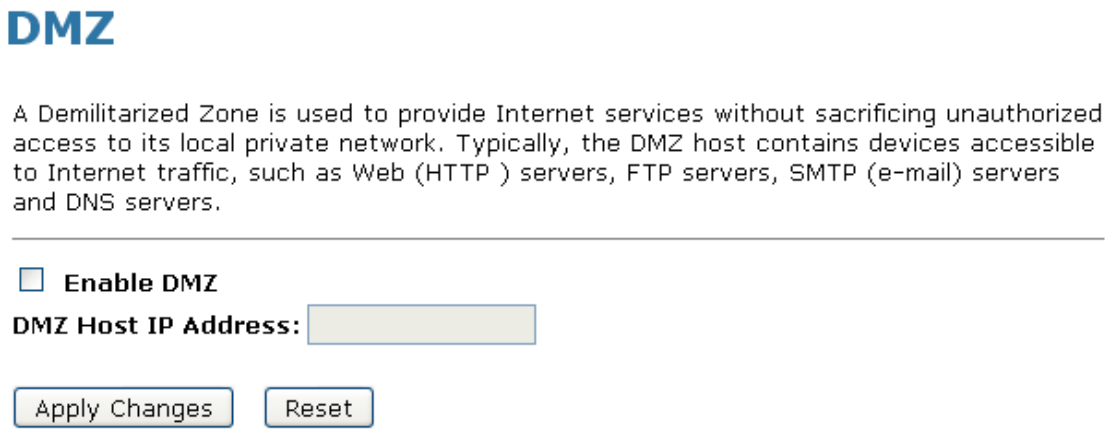


5. Il filtro creato viene automaticamente aggiunto alla *Current Filter Table*.
6. In tal modo l'URL inserito non è più accessibile agli utenti della rete LAN.

17 DMZ

Una zona definita demilitarizzata (DMZ - Demilitarized Zone) si utilizza per fornire servizi Internet senza sacrificare accessi non autorizzati alla rete locale privata. Tipicamente, l'host DMZ contiene dispositivi accessibili al traffico Internet, quali WEB server (HTTP), Server FTP, Server SMTP (e-mail) e Server DNS.

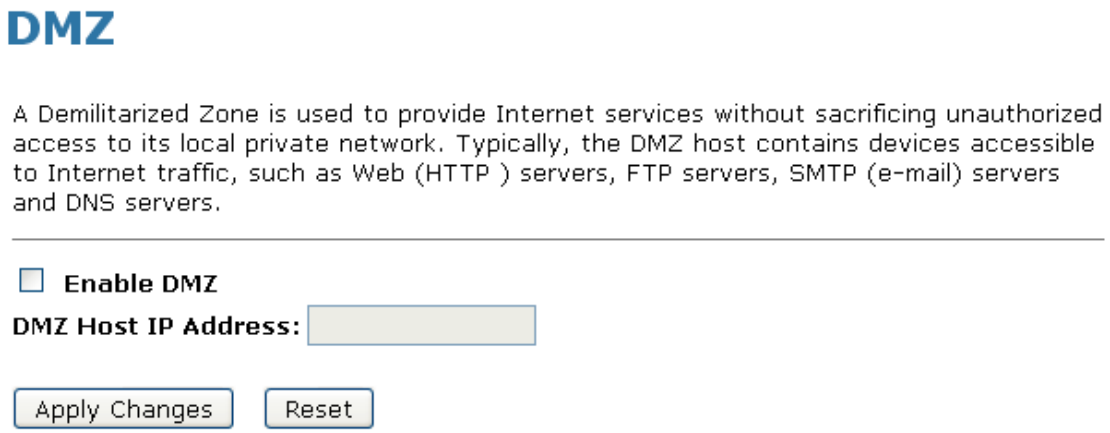
1. Dal menù di sinistra, selezionare *Firewall -> DMZ*. Si visualizza la seguente pagina:


DMZ
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
Enable DMZ
DMZ Host IP Address:
Apply Changes
Reset

Indirizzo IP dell'Host DMZ

Si faccia riferimento all'esempio sottostante per configurare l'indirizzo IP dell'Host DMZ.

1. Dal menù di sinistra, selezionare *Firewall -> DMZ*. Si visualizza la seguente pagina:


DMZ
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
Enable DMZ
DMZ Host IP Address:
Apply Changes
Reset

2. Verificare che l'opzione *Enable DMZ* sia abilitata.
3. Digitare l'indirizzo IP da assegnare all'Host DMZ nel campo *DMZ Host IP Address*.
4. Premere il pulsante *Apply Changes*.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Enable DMZ

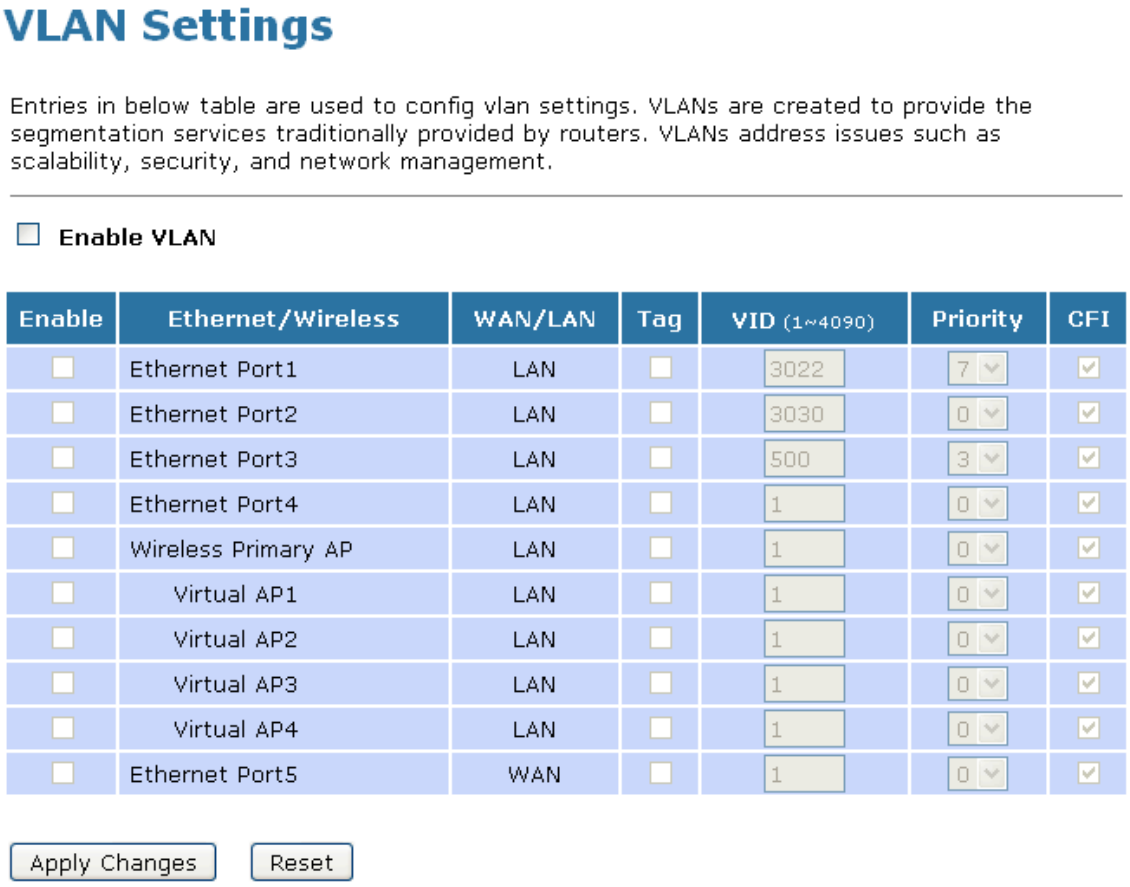
DMZ Host IP Address: 10.0.0.101

Apply Changes Reset

18 VLAN

I valori della tabella sottostante sono necessari per configurare le VLAN. Le VLAN sono necessarie per il servizio di segmentazione tradizionalmente fornito dai router e permettono di gestire funzionalità quali la scalabilità, la sicurezza e la gestione della rete.

1. Dal menù di sinistra, selezionare *Firewall -> VLAN*. Si visualizza la seguente pagina:



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

Enable VLAN

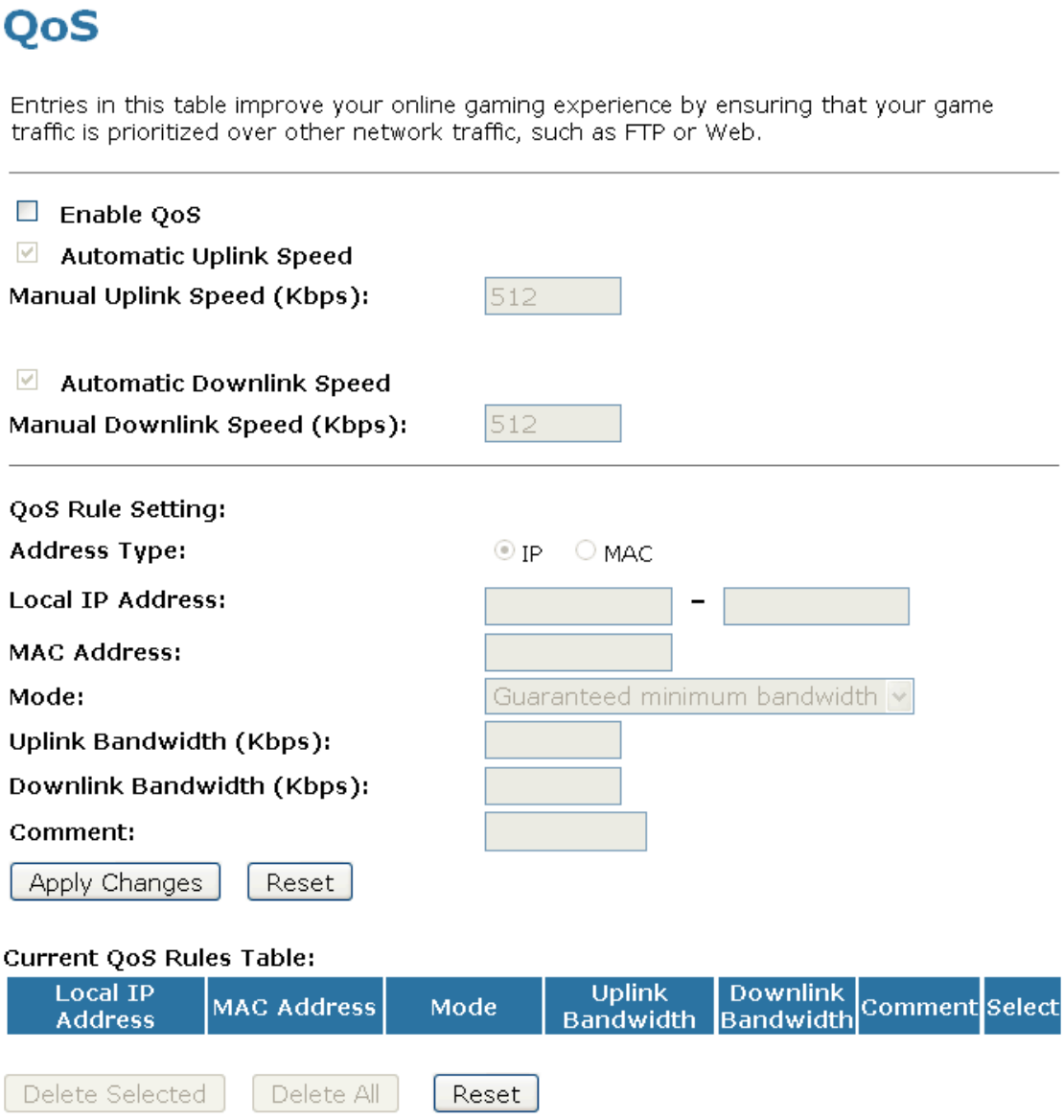
Enable	Ethernet/Wireless	WAN/LAN	Tag	VID (1~4090)	Priority	CFI
☐	Ethernet Port1	LAN	☐	3022	7	☑
☐	Ethernet Port2	LAN	☐	3030	0	☑
☐	Ethernet Port3	LAN	☐	500	3	☑
☐	Ethernet Port4	LAN	☐	1	0	☑
☐	Wireless Primary AP	LAN	☐	1	0	☑
☐	Virtual AP1	LAN	☐	1	0	☑
☐	Virtual AP2	LAN	☐	1	0	☑
☐	Virtual AP3	LAN	☐	1	0	☑
☐	Virtual AP4	LAN	☐	1	0	☑
☐	Ethernet Port5	WAN	☐	1	0	☑

Apply Changes Reset

19 QoS

I valori di questa tabella possono migliorare le vostre esperienze di gioco, assicurando che le comunicazioni dei giochi siano prioritarie rispetto il restante traffico di rete, quale FTP o WEB.

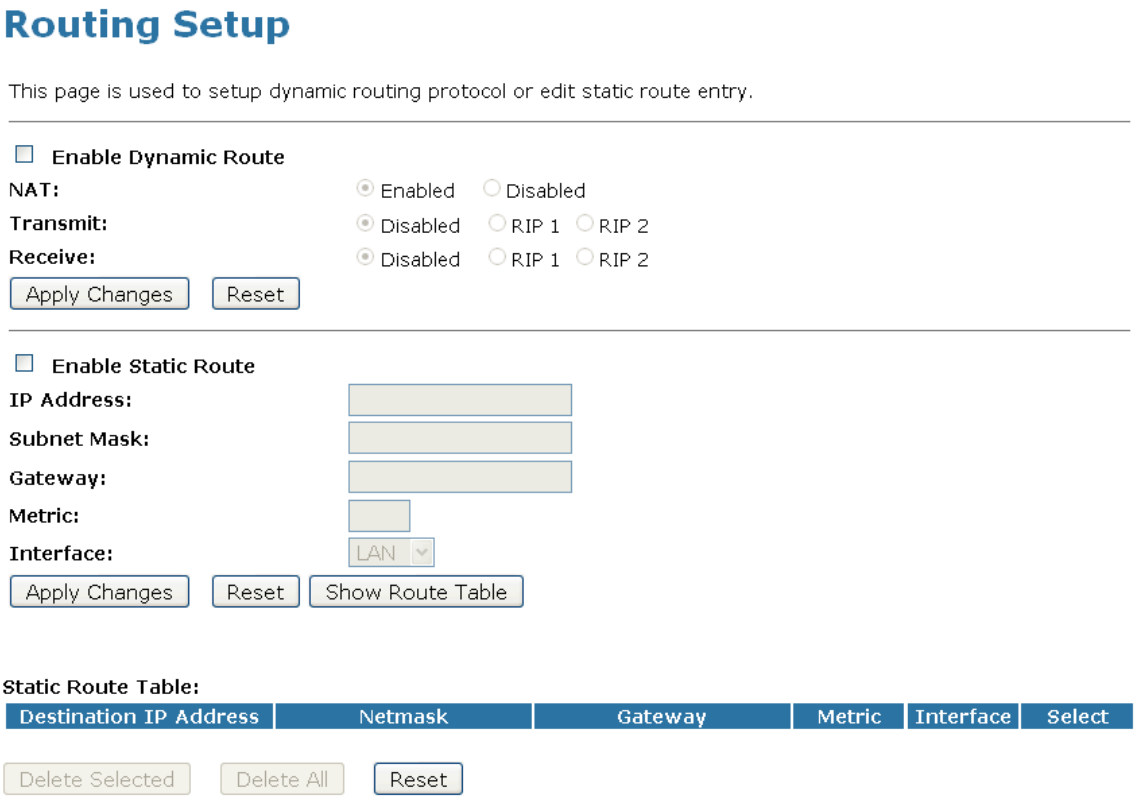
1. Dal menù di sinistra, selezionare *Firewall -> QoS*. Si visualizza la seguente pagina:



20 Route Setup

Questa pagina permette di configurare i parametri per la configurazione del protocollo per il routing dinamico o statico.

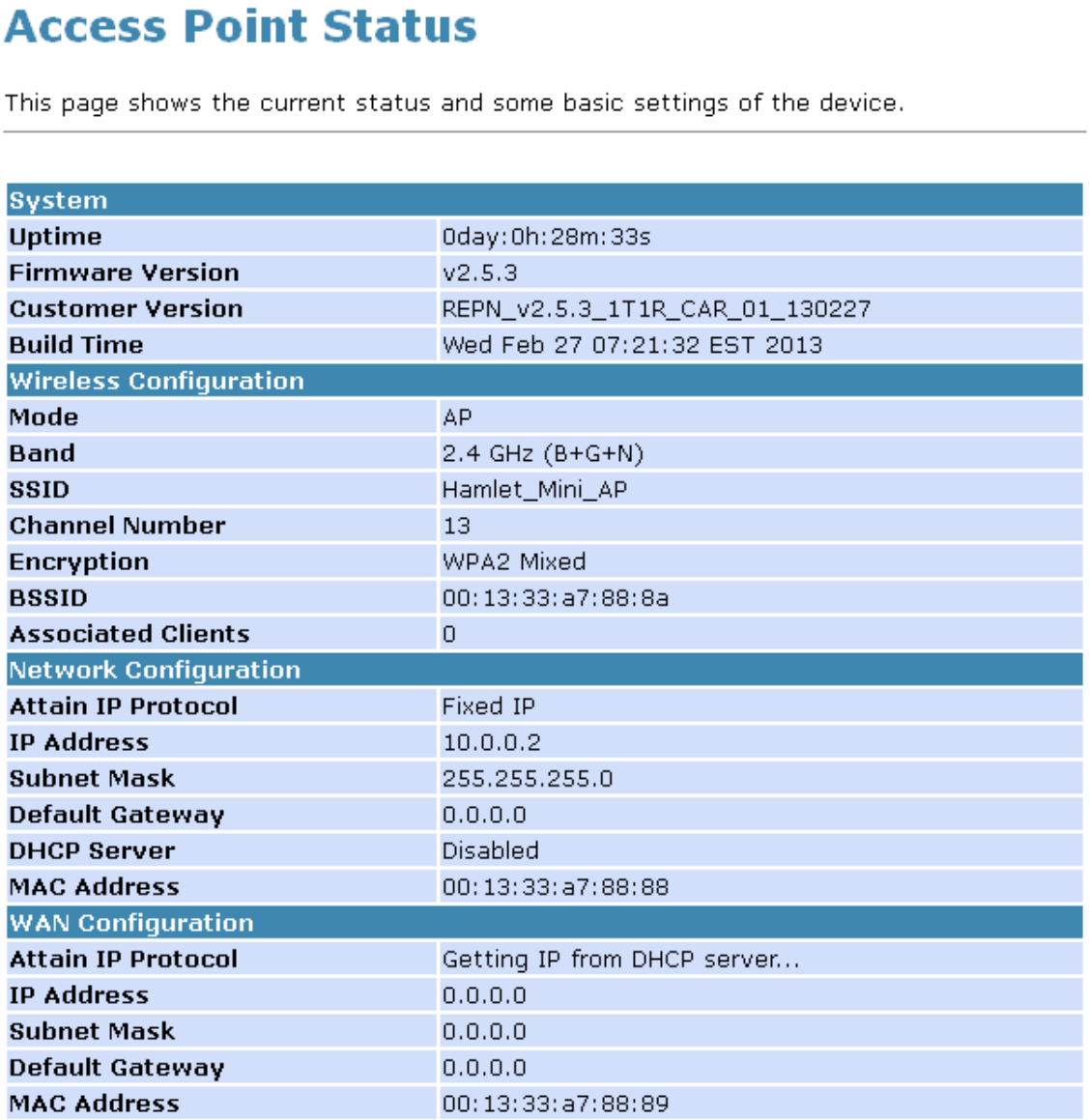
1. Dal menù di sinistra, selezionare *Route Setup*. Si visualizza la seguente pagina:


Routing Setup
This page is used to setup dynamic routing protocol or edit static route entry.
Enable Dynamic Route
NAT: Enabled Disabled
Transmit: Disabled RIP 1 RIP 2
Receive: Disabled RIP 1 RIP 2
Apply Changes Reset
Enable Static Route
IP Address:
Subnet Mask:
Gateway:
Metric:
Interface: LAN
Apply Changes Reset Show Route Table
Static Route Table:
Destination IP Address Netmask Gateway Metric Interface Select
Delete Selected Delete All Reset

21 Stato del dispositivo

La pagina visualizza lo stato attuale del dispositivo. In particolare sono visualizzati i dati relativi alla LAN, WAN ed al Firmware del sistema. Si noti che le informazioni visualizzate variano in funzione della configurazione della WAN (IP statico, DHCP o PPPoE).

1. Dal menù di sinistra, selezionare *Management -> Status*. Si visualizza la seguente pagina:



Access Point Status

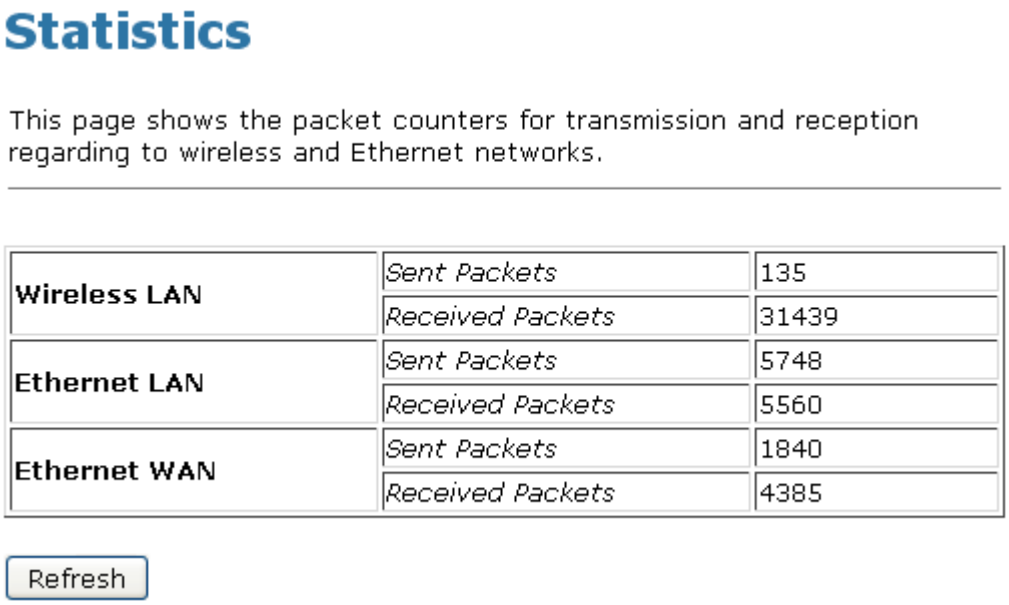
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:28m:33s
Firmware Version	v2.5.3
Customer Version	REPN_v2.5.3_1T1R_CAR_01_130227
Build Time	Wed Feb 27 07:21:32 EST 2013
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	Hamlet_Mini_AP
Channel Number	13
Encryption	WPA2 Mixed
BSSID	00:13:33:a7:88:8a
Associated Clients	0
Network Configuration	
Attain IP Protocol	Fixed IP
IP Address	10.0.0.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:13:33:a7:88:88
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:13:33:a7:88:89

22 Statistiche

La pagina visualizza i contatori dei pacchetti dati trasmessi o ricevuti sia sulla rete Wireless che la rete Ethernet.

1. Dal menù di sinistra, selezionare *Management -> Statistics*. Si visualizza la seguente pagina:



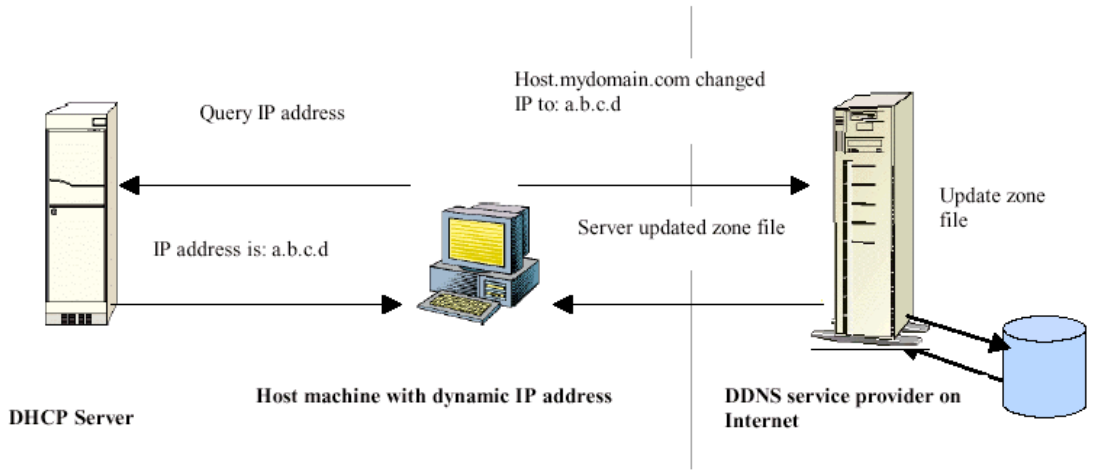
23 DNS Dinamico

Qualora si utilizzi il server interno come Server DNS, anziché utilizzare l'assegnazione dinamica dell'indirizzo IP, si può utilizzare il servizio DDNS. Il servizio DDNS permette di simulare un indirizzo IP dinamico su un indirizzo IP statico.

Il presente capitolo fornisce una panoramica del servizio DNS Dinamico del modem e le modalità per le procedure per configurare tale servizio.

Generalità

Se l'host viene identificato con un indirizzo IP dinamico che cambia frequentemente, risulterà difficoltoso mantenere aggiornato il record IP associato al nome a dominio dell'host nei file di zona. Ciò renderà l'accessibilità dell'host da Internet difficile se non impossibile. Il servizio DNS Dinamico ha quindi il compito di mantenere aggiornata la mappa degli indirizzi IP dinamici assegnati all' Host riferendoli ad un hostname statico. Servizi di DNS Dinamico sono resi disponibili da vari siti Web. L'Host deve essere registrato con alcuni siti WEB a prendere un nome a dominio. Quando cambia l'indirizzo IP dell'host, sarà sufficiente inviare un messaggio al sito WEB che fornisce il servizio di DNS Dinamico. Per tale operazione si rende quindi necessario implementare un sistema client per l'aggiornamento automatico. Il sistema di aggiornamento dovrà inviare un messaggio al server ogni qualvolta si verifichi un cambiamento all'indirizzo IP dell'host. Alla ricezione del messaggio, il server provvederà quindi ad aggiornare il report IP dell'host e a reinviare al client alcuni codici di risposta.



La precedente figura illustra un possibile scenario in cui un Host prende un indirizzo IP dinamico da un server DHCP. Quando l'Host è registrato ad un servizio DNS dinamico su uno dei provider disponibili in Internet, l'host deve inviare al provider un messagio con il proprio hostname e l'indirizzo IP cambiato. Il provider del servizio aggiorna il nuovo indirizzo IP dell'host nei file di zona relativi e risponde al messaggio con alcuni codici di risposta. I codici di risposta indicano se l'operazione di aggiornamento ha avuto successo o meno. Tale operazione si ripete ogni volta che cambia l'indirizzo IP assegnato all'host.

Se il servizio di DNS dinamico riceve ripetutamente messaggi di aggiornamento, tale condizione verrà considerata come un abuso causando il blocco dell'hostname. Per evitare il verificarsi di tale condizione, quando l'indirizzo IP viene aggiornato dall'ISP, viene anche registrato nel dispositivo. Quando si riceve una notifica di assegnazione dell'indirizzo IP, il nuovo IP viene innanzitutto verificato con l'ultimo indirizzo IP segnalato al servizio DNS dinamico. Se l'indirizzo IP è differente, viene generato un messaggio di aggiornamento. Tuttavia, quando si avvia il sistema non c'è possibilità di conoscere quale era l'indirizzo IP assegnato prima che il sistema fosse spento. E'

quindi necessario inviare periodicamente il comando “system config save“ per salvare l'indirizzo IP nella memoria flash.

Registrazione su un Provider del servizio DNS Dinamico

Attualmente, il router supporta due provider del servizio DNS dinamico: www.tzo.com e www.dyndns.com. Per utilizzare il loro servizio è necessario consultare il loro sito WEB e provvedere alla registrazione del proprio host. Durante la registrazione, si dovrà fornire il proprio username, la password e l' hostname come parametri obbligatori. Il fornitore del servizio può comunque richiedere ulteriori parametri opzionali.

Configurazione delle interfacce IP

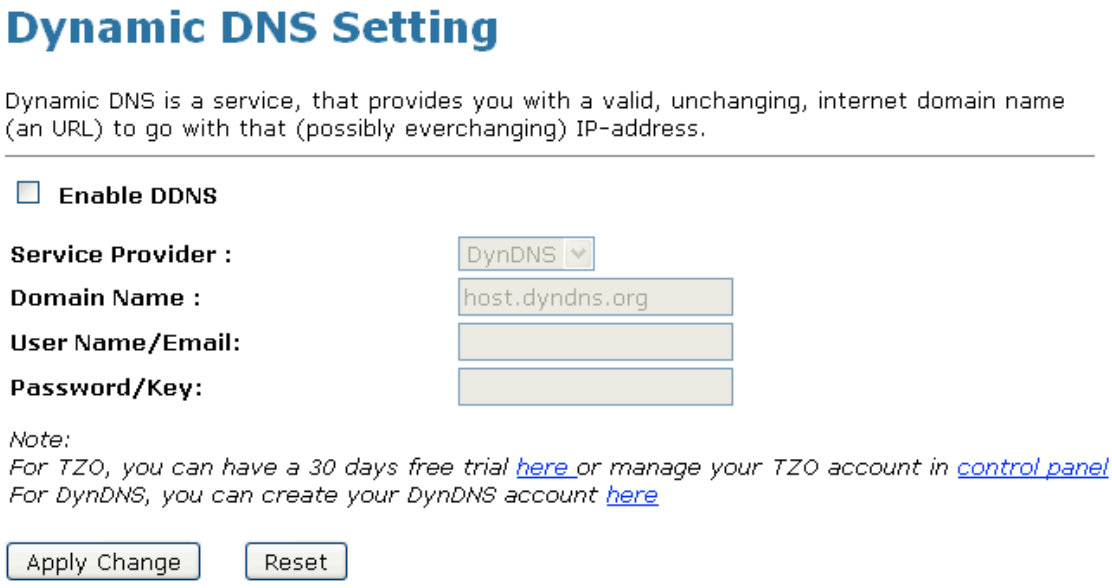
E' necessario creare una interfaccia DNS dinamica per l'interfaccia IP ed è possibile creare un solo servizio DNS Dinamico per una interfaccia IP. Per ulteriori informazioni sulla modalità di creazione delle interfacce IP fa riferimento alla sezione 'Creare Interfacce IP'.

Nota

www.dyndns.org fornisce tre tipi di servizi: DNS Dinamico, DNS Custom e DNS Statico. Su questo sistema si possono creare differenti domini. Il servizio DNS Custom è una soluzione completa per nuovi domini o domini già esistenti. Una interfaccia di tipo Web permette il controllo delle risorse di registrazione e per la gestione dell'intero dominio, inclusi i supporti per gli IP dinamici e gli aggiornamenti automatici. Il servizio di DNS Statico punta un hostname DNS di alcuni domini proprietari di dyndns.org all'indirizzo IP statico o pseudo-statico assegnato dall'ISP all'utente.

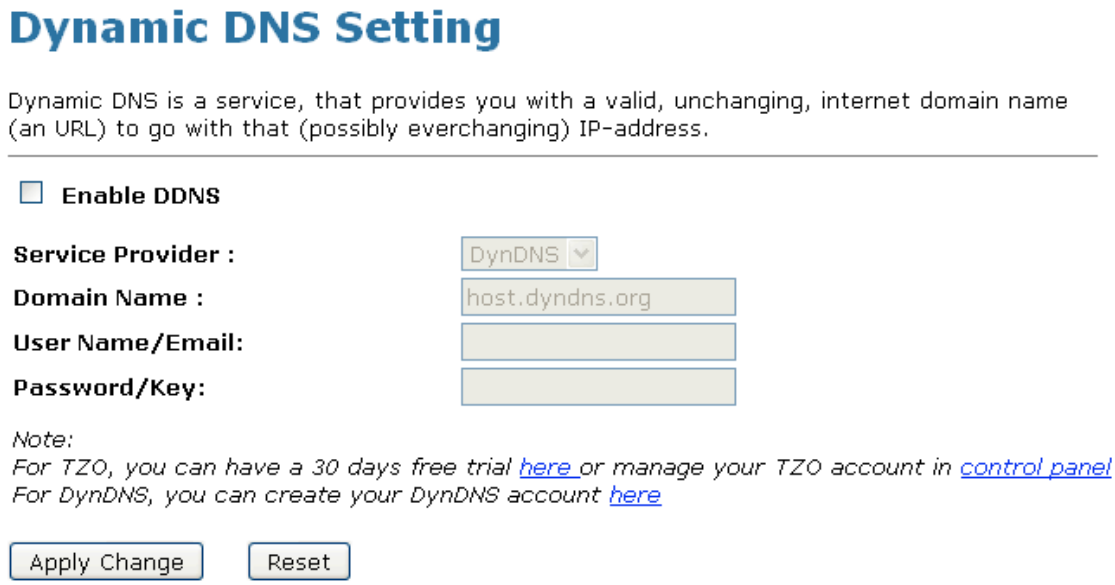
Il servizio DynDNS punta un hostname fisso di alcuni domini proprietari di dyndns.org all'indirizzo IP assegnato dall'ISP all'utente. Questo permette aggiornamenti più frequenti degli indirizzi IP rispetto al DNS Statico.

1. Dal menù di sinistra, selezionare *Management -> DDNS*. Si visualizza la seguente pagina:

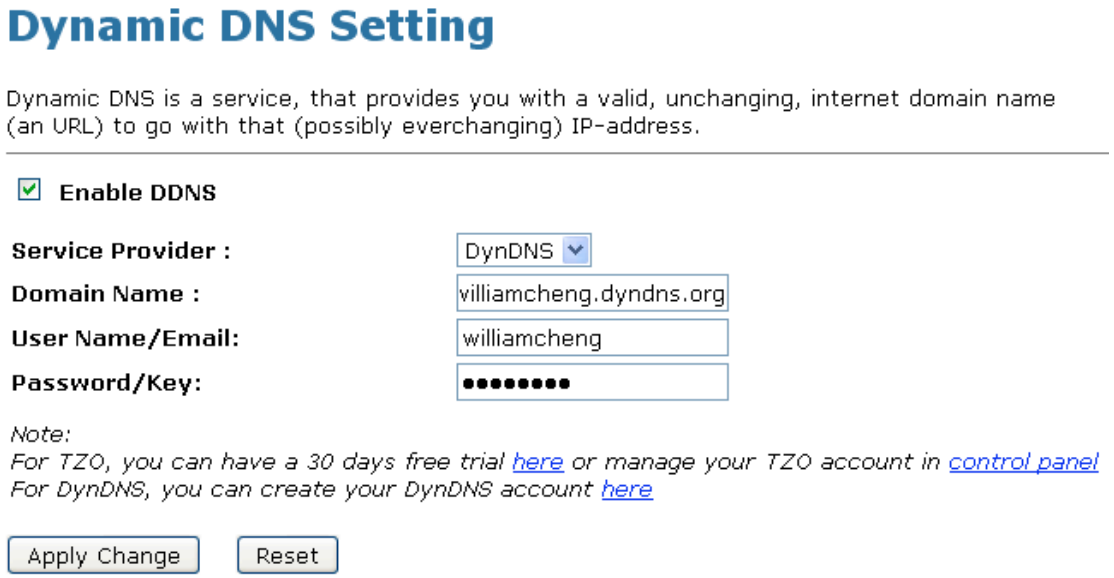

Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
DynDNS
Domain Name :
host.dyndns.org
User Name/Email:
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

Configurare DynDNS

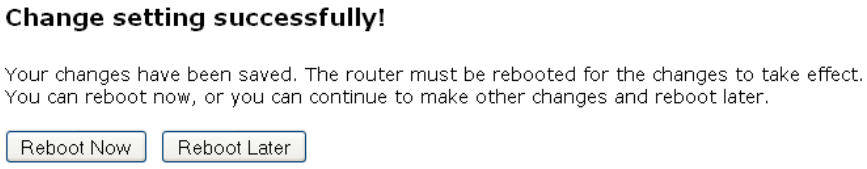
2. Dal menù di sinistra, selezionare *Management -> DDNS*. Si visualizza la seguente pagina:


Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
DynDNS
Domain Name :
host.dyndns.org
User Name/Email:
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

3. Premere il pulsante *Enable DDNS*
4. Selezionare l'opzione *DynDNS* dall'elenco del campo *Service Provider*.
5. Digitare i propri Username, Password e nome del dominio per il servizio di www.dyndns.com nei relativi Campi. Possono essere una qualsiasi combinazione di lettere e numeri con lunghezza massima di 20 caratteri.
6. Premere il pulsante *Apply Changes*.

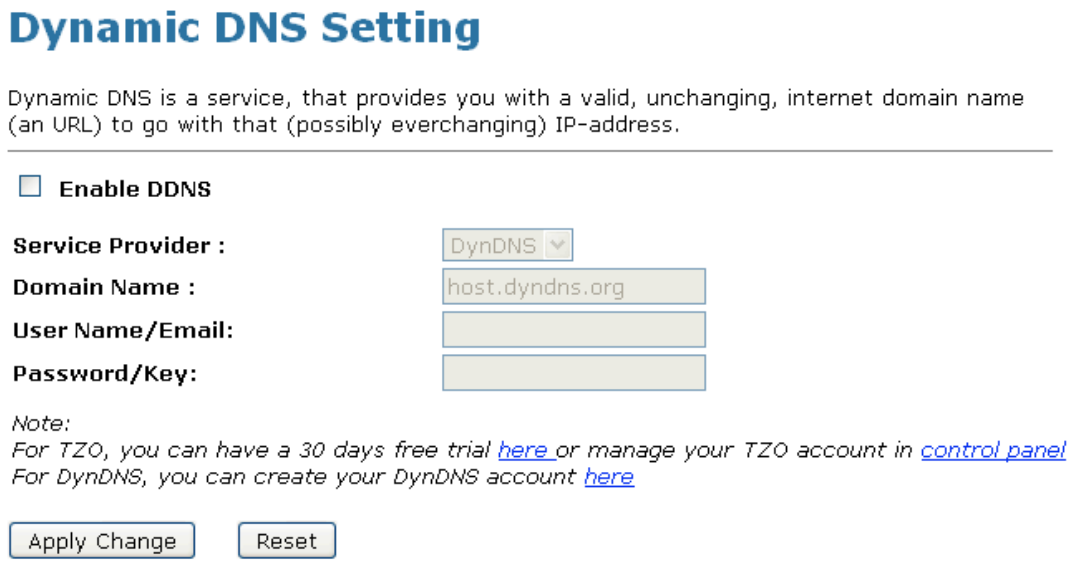

Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
DynDNS
Domain Name :
villiamcheng.dyndns.org
User Name/Email:
williamcheng
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

7. *Le modifiche sono state correttamente effettuate!*
   Premere il pulsante *Reboot Now* per confermare.

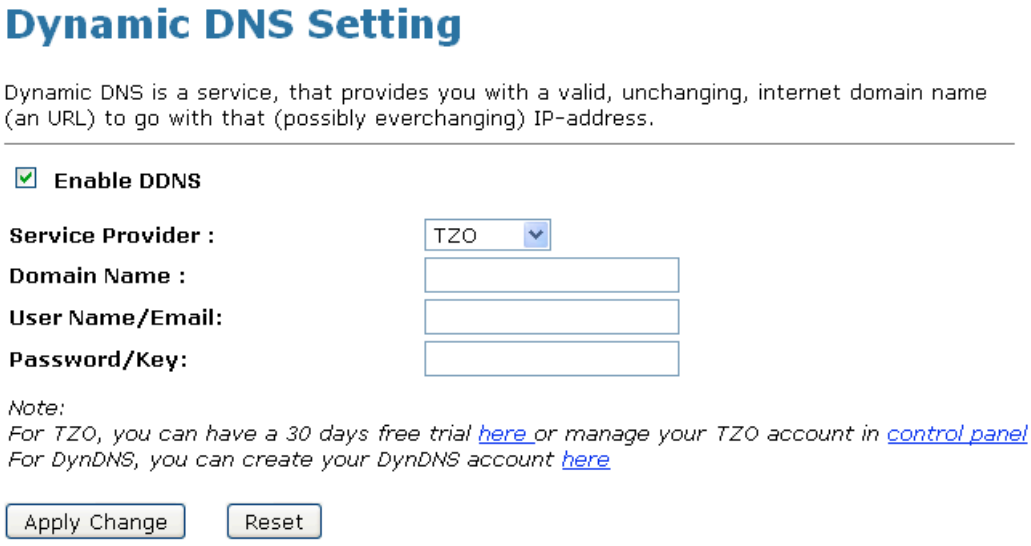

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

Configurazione TZO

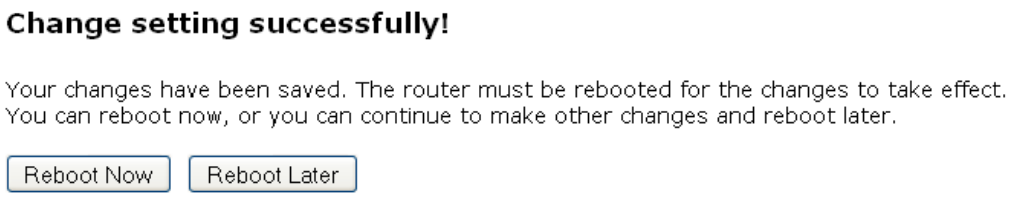
1. Dal menù di sinistra, selezionare *Management -> DDNS*. Si visualizza la seguente pagina:


Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
DynDNS
Domain Name :
host.dyndns.org
User Name/Email:
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

2. Premere il pulsante *Enable DDNS*
3. Selezionare l'opzione *TZO* dall'elenco del campo *Service Provider*.
4. Digitare la propria Email, il codice ed il nome del dominio che si sono utilizzati nella pagina http://www.tzo.com/MainPageWebClient/clientsignup.html nei rispettivi campi. I valori possono essere una qualsiasi combinazione di lettere e numeri con lunghezza massima di 20 caratteri.
5. Premere il pulsante *Apply Changes*.


Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
TZO
Domain Name :
User Name/Email:
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

6. *Le modifiche sono state correttamente effettuate!* Premere *Reboot Now* per confermare.

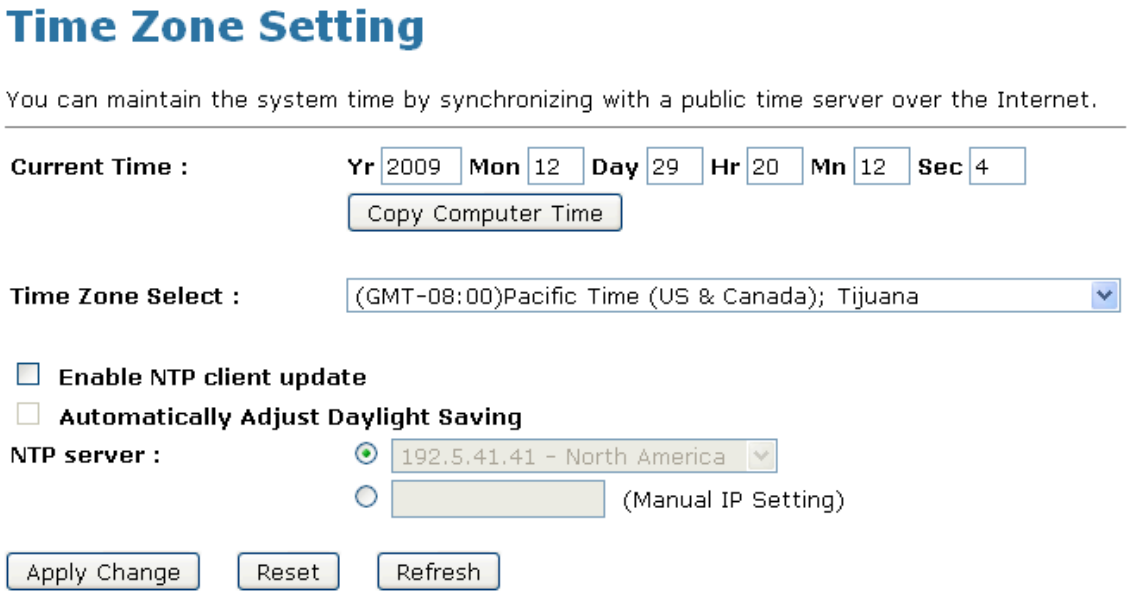

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

24 Configurazione Time Zone

Alcuni sistemi potrebbero non avere un orologio di sistema (data ed ora) oppure potrebbero utilizzare un orologio di sistema il cui orario non è sufficientemente accurato. La funzione di Simple Network Time Protocol (SNTP) fornisce un mezzo per sincronizzare l'orologio del dispositivo con un server remoto, così come specificato negli standard RFC 2030 (SNTP) e RFC 1305 (NTP).

Configurazione del Server SNTP e del Client SNTP

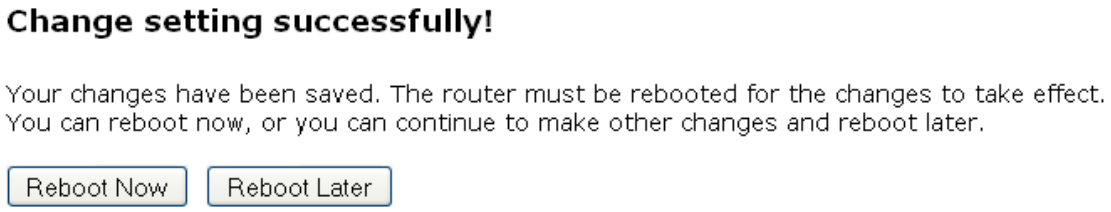
1. Dal menù di sinistra selezionare *Time Zone Setting*. Si visualizza la seguente pagina:


Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2009 Mon 12 Day 29 Hr 20 Mn 12 Sec 4
Copy Computer Time
Time Zone Select :
(GMT-08:00)Pacific Time (US & Canada); Tijuana
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

2. Dall'elenco predefinito del campo *Time Zone Select*, selezionare la propria zona oraria di appartenenza.
3. Selezionare l'opzione *Enable NTP client update*.
4. Selezionare dall'elenco del campo *NTP server* uno degli NTP server disponibili. Oppure, è possibile aggiungere un server all'elenco dei Server SNTP digitando il relativo indirizzo IP. Aggiungendo un server alla lista, automaticamente inizia la sincronizzazione oraria.
5. Premere il pulsante *Apply Changes*.

Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2009 Mon 12 Day 29 Hr 20 Mn 12 Sec 4
Copy Computer Time
Time Zone Select :
(GMT-08:00)Pacific Time (US & Canada); Tijuana
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

6. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

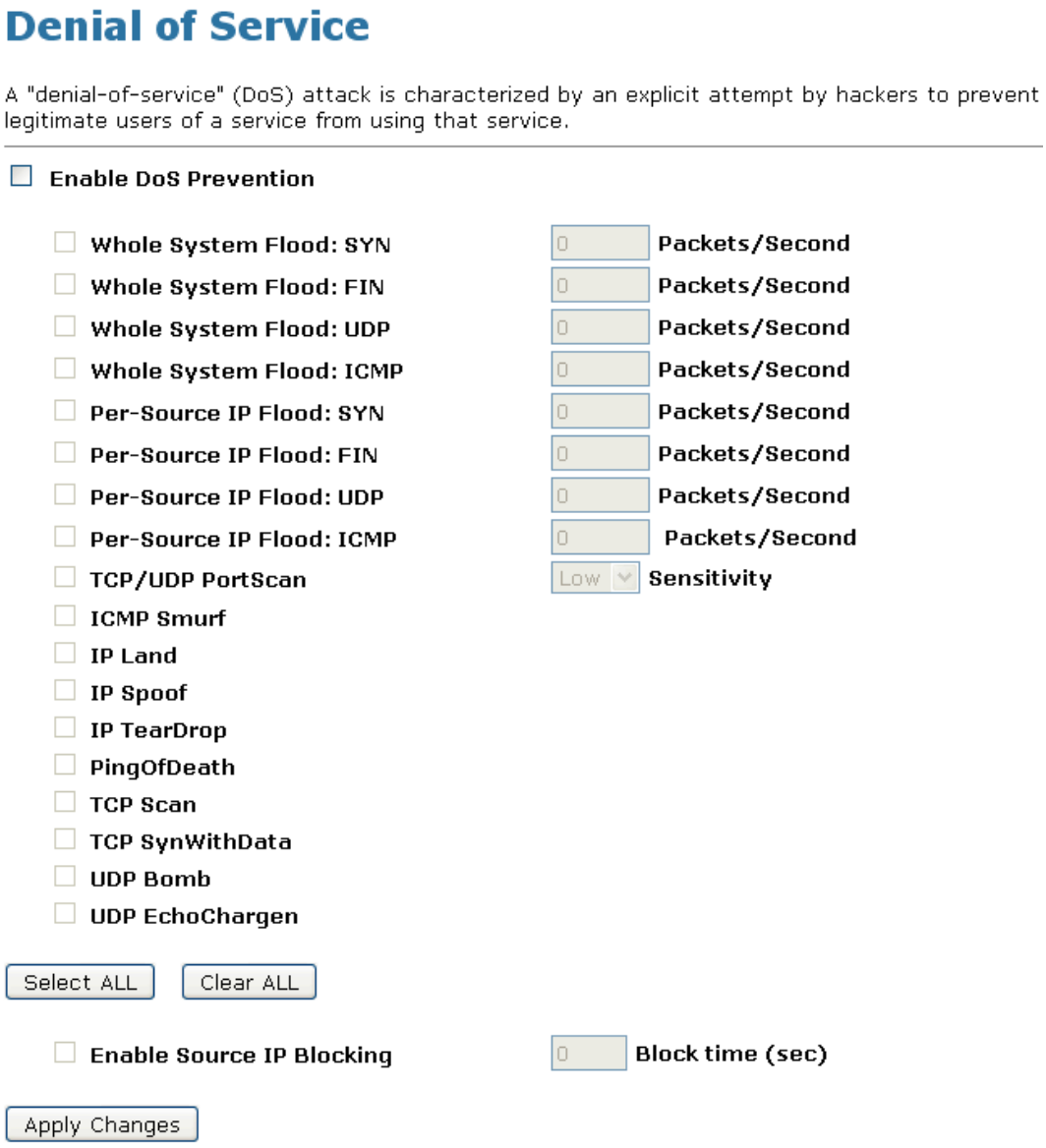

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

25 Denial-of-Service

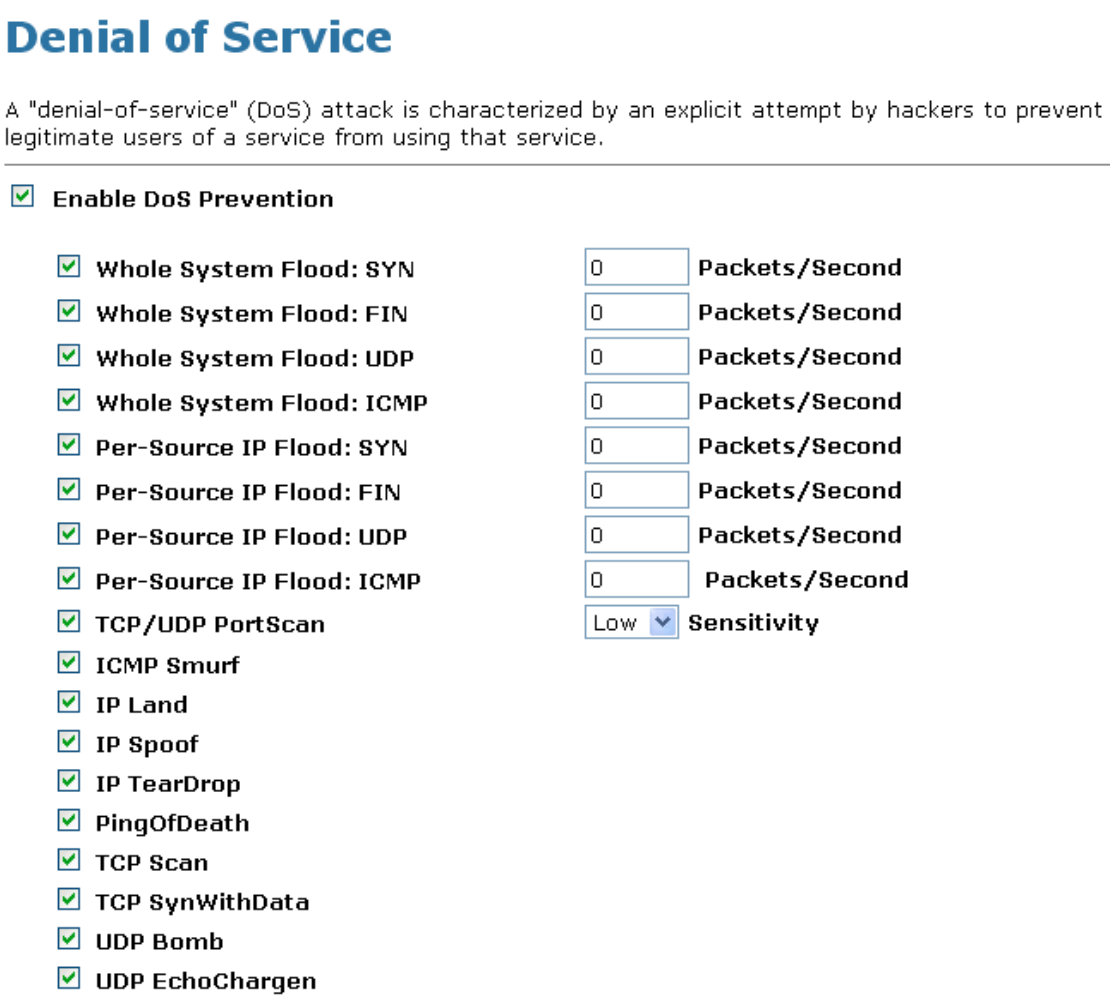
Un attacco definito "denial-of-service" (DoS) è caratterizzato da un tentativo degli hacker di far si che utenti legittimati all'uso di un servizio non possano più usarlo.

Denial-of-Service

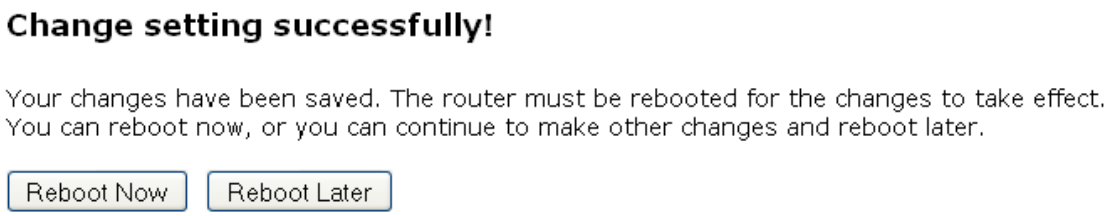
1. Dal menù di sinistra, selezionare *Denial-of-Service*. Si visualizza la seguente pagina:


Denial of Service
A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.
Enable DoS Prevention
Whole System Flood: SYN 0 Packets/Second
Whole System Flood: FIN 0 Packets/Second
Whole System Flood: UDP 0 Packets/Second
Whole System Flood: ICMP 0 Packets/Second
Per-Source IP Flood: SYN 0 Packets/Second
Per-Source IP Flood: FIN 0 Packets/Second
Per-Source IP Flood: UDP 0 Packets/Second
Per-Source IP Flood: ICMP 0 Packets/Second
TCP/UDP PortScan Low Sensitivity
ICMP Smurf
IP Land
IP Spoof
IP TearDrop
PingOfDeath
TCP Scan
TCP SynWithData
UDP Bomb
UDP EchoChargen
Select ALL
Clear ALL
Enable Source IP Blocking 0 Block time (sec)
Apply Changes

2. Selezionare l'opzione *Enable NTP client update*.
3. Selezionare l'opzione di ciascun servizio.
4. Verificare che l'opzione *Enable Source IP Blocking* sia abilitata.
5. Premere il pulsante *Apply Changes*.


Denial of Service
A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.
Enable DoS Prevention
Whole System Flood: SYN 0 Packets/Second
Whole System Flood: FIN 0 Packets/Second
Whole System Flood: UDP 0 Packets/Second
Whole System Flood: ICMP 0 Packets/Second
Per-Source IP Flood: SYN 0 Packets/Second
Per-Source IP Flood: FIN 0 Packets/Second
Per-Source IP Flood: UDP 0 Packets/Second
Per-Source IP Flood: ICMP 0 Packets/Second
TCP/UDP PortScan Low Sensitivity
ICMP Smurf
IP Land
IP Spoof
IP TearDrop
PingOfDeath
TCP Scan
TCP SynWithData
UDP Bomb
UDP EchoChargen
Select ALL
Clear ALL
Enable Source IP Blocking 0 Block time (sec)
Apply Changes

6. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.

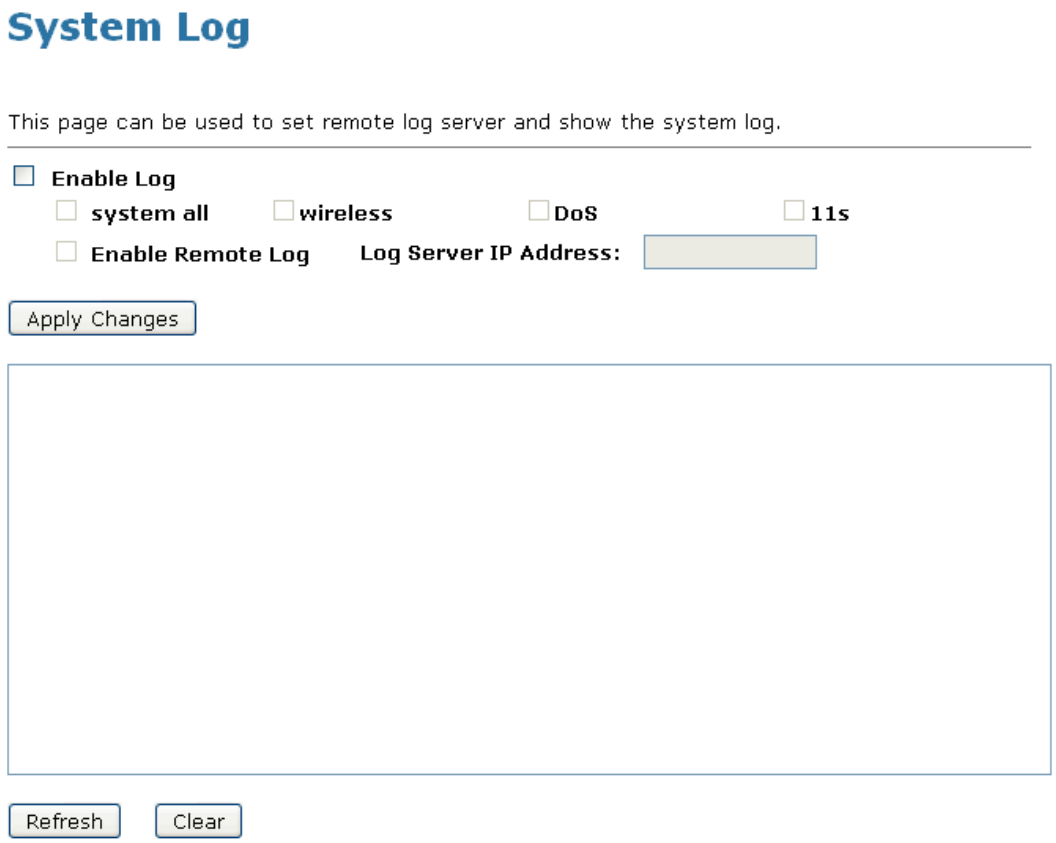

Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

26 Log

Questa schermata può essere utilizzata per impostare il server di log remoto e visualizzare il log di sistema.

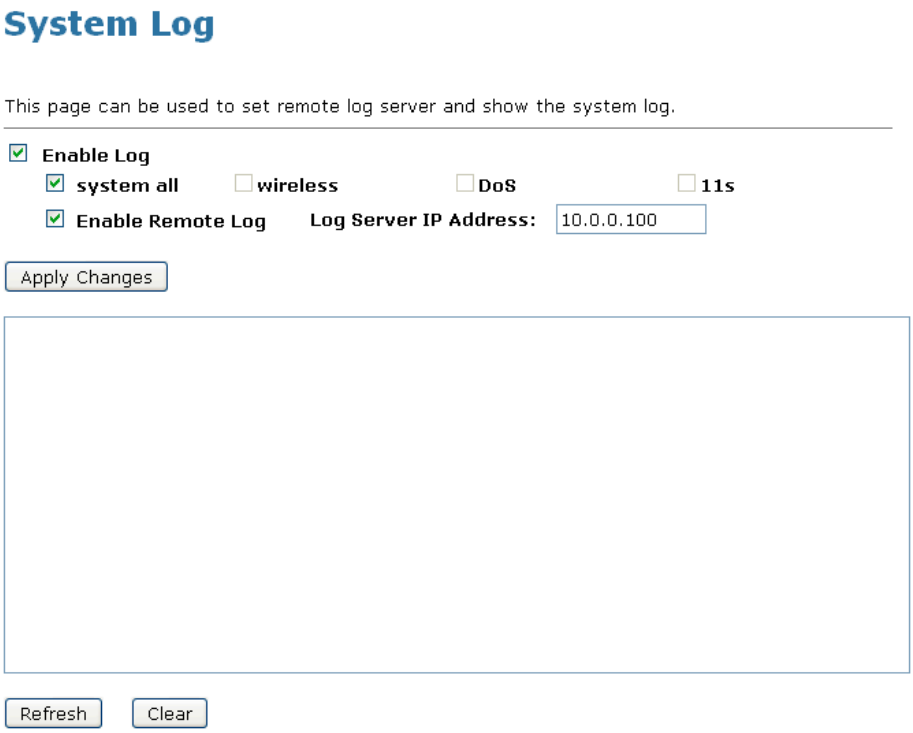
Log di sistema

1. Dal menù di sinistra, selezionare *Log*. Si visualizza la seguente pagina:

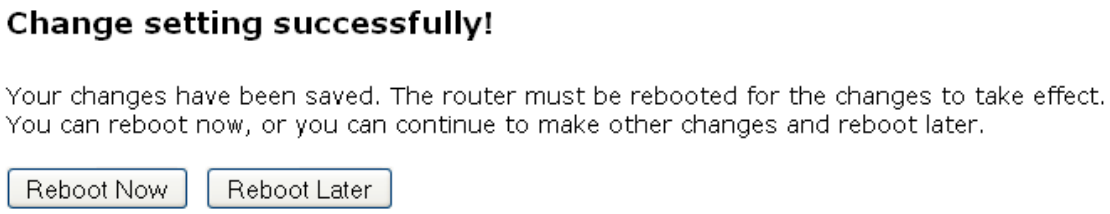


Opzioni	Descrizione
Enable Log	Abilita/disabilita la funzione. Default: Disabilitata
system all	Tutti i log saranno registrati nel log di sistema
wireless	I log della rete wireless saranno registrati nel log di sistema
DoS	I log della funzione DoS saranno registrati nel log di sistema
Enable Remote Log	Invia il log di sistema ad un server remoto preposto per il log. Per fare questo, assicurarsi che sia disponibile un server sicuro abilitato al log di sistema. Default: Disabilitata
Log Server IP Address	Digitare l'indirizzo IP del Server remoto di log.

2. Abilitare l'opzione *Enable Log*.
3. Abilitare l'opzione *system all*, *wireless* o *DoS*.
4. Abilitare l'opzione *Enable Remote Log*, se si vuole attivare la funzione
5. Digitare l'indirizzo IP del Server di Log nel campo *Log Server IP Address*.
6. Premere il pulsante *Apply Changes*.



7. Si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Premere il pulsante *Reboot Now* per confermare.


Change setting successfully!
Your changes have been saved. The router must be rebooted for the changes to take effect.
You can reboot now, or you can continue to make other changes and reboot later.
Reboot Now
Reboot Later

27 Aggiornamento Firmware

Informazioni utili circa la versione firmware

Il firmware è il software con cui opera il dispositivo. Ed è memorizzato nella memoria di sola lettura del dispositivo.

Il Router può verificare quando una nuova versione di firmware è resa disponibile. Se è disponibile una nuova versione, è possibile scaricarla via Internet ed installarla sul dispositivo.

Nota

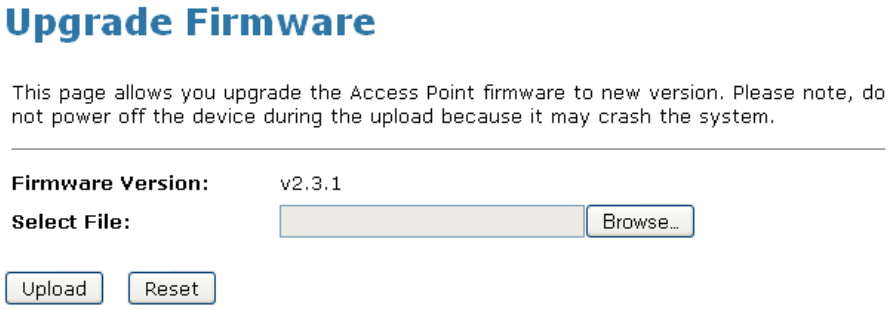
In presenza di una nuova versione del firmware, si consiglia vivamente di installarla quanto prima, così di assicurarsi tutti i vantaggi degli aggiornamenti e delle nuove funzionalità implementate.

Aggiornamento manuale del firmware

Si può eseguire il download manuale dell'ultima versione del firmware, scaricandolo dal sito del costruttore e salvandolo in una cartella del PC.

Dopo aver scaricato la versione più aggiornata del firmware, è possibile installarlo manualmente nel seguente modo:

1. Dal menù di sinistra selezionare *Upgrade Firmware Upgrade*. Si visualizza la seguente pagina:
2. Premere il pulsante *Browse…* .

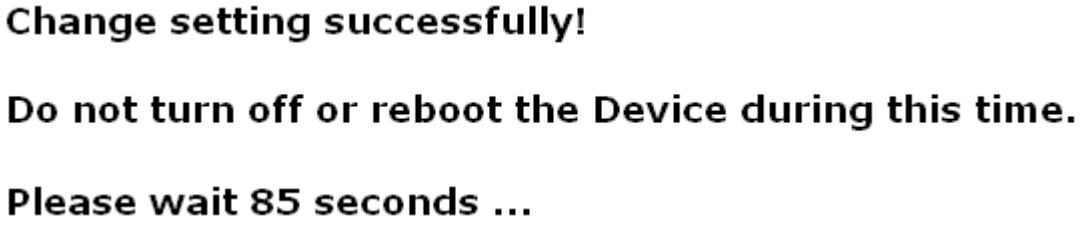

Upgrade Firmware
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.
Firmware Version:
v2.3.1
Select File:
Browse...
Upload
Reset

(Si noti che utilizzando alcuni browser (ad esempio Opera 7) il pulsante può essere denominato Choose..)

Utilizzare la finestra di selezione del file per sezionare la cartella in cui si è salvato il file contenente la versione aggiornata del firmware.

3. Dopo aver selezionato il file, premere il pulsante Open. Il percorso del file verrà visualizzato nel campo *New Firmware Image:*.
4. Premere il pulsante *Upload*. Il dispositivo verifica che il file contenga una versione più aggiornata e quindi segnala l'avvio dell'aggiornamento.

5. Al termine, quando l'aggiornamento del firmware è stato completato, si visualizza il seguente messaggio:
   Le modifiche sono state correttamente effettuate!
   Non spegnere o riavviare il dispositivo.
   Attendere 85 secondi ...



28 Salvataggio/Lettura della configurazione

Questa pagina consente di salvare in un file i dati di configurazione ovvero di rileggere i dati di configurazione da un file precedentemente salvato.

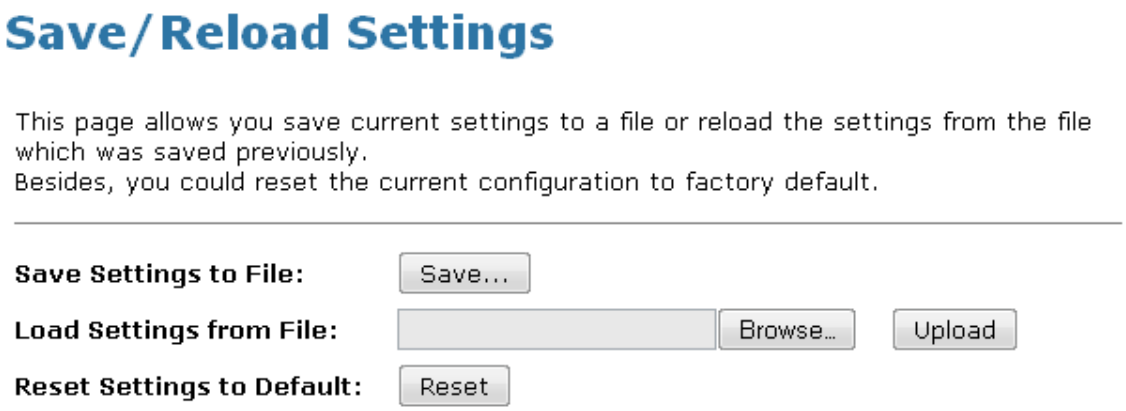
Altresì, dalla pagina è possibile ripristinare la configurazione ai valori di fabbrica.

Qualora si siano effettuate modifiche alla configurazione e si voglia ritornare alla configurazione iniziale del dispositivo, questo può essere fatto ripristinando i valori di default impostati in fabbrica.

Salvataggio della configurazione in un file

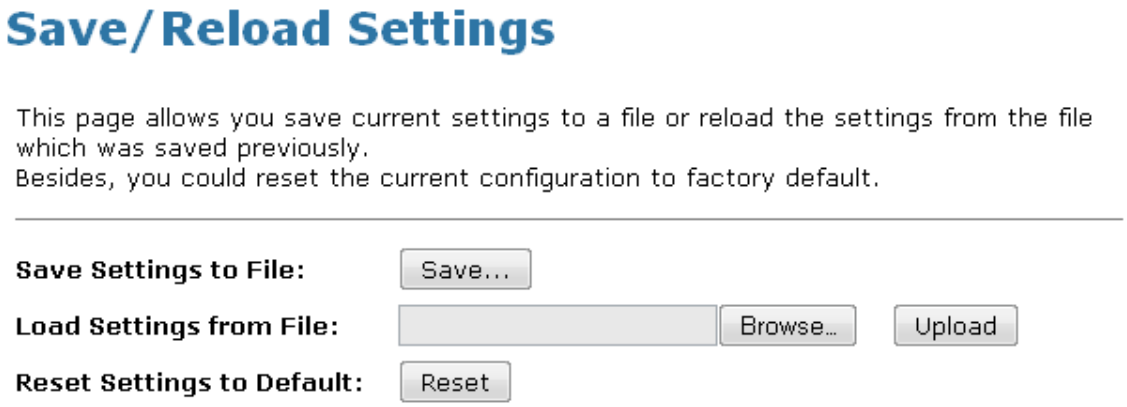
Tale operazione permette di salvare tutti i dati di configurazione in un file.

1. Dal menù di sinistra selezionare *Reset factory default*. Si visualizza la seguente pagina:

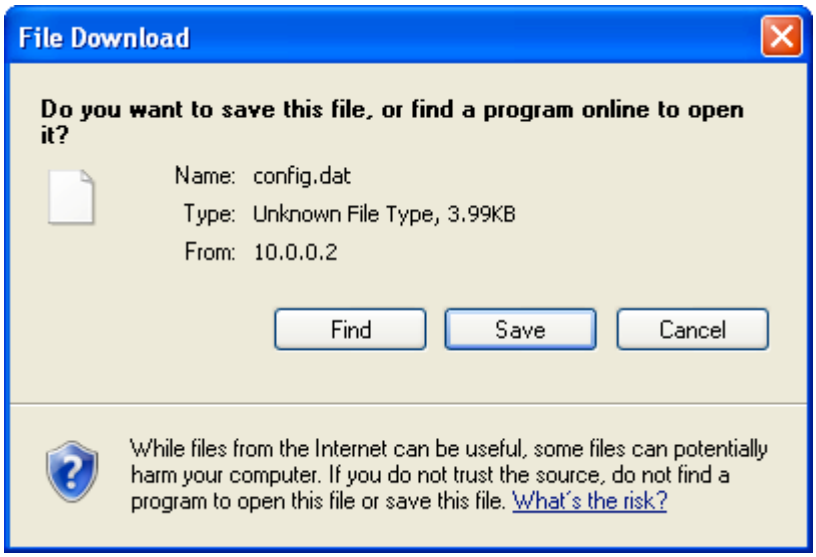

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

Opzione	Descrizione
Save Settings to File	Salvataggio della configurazione in un file
Load Settings from File	Legge la configurazione da un file
Reset Settings to Default	Ripristina i valori di default impostati in fabbrica

2. Premere il pulsante *Save*….


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

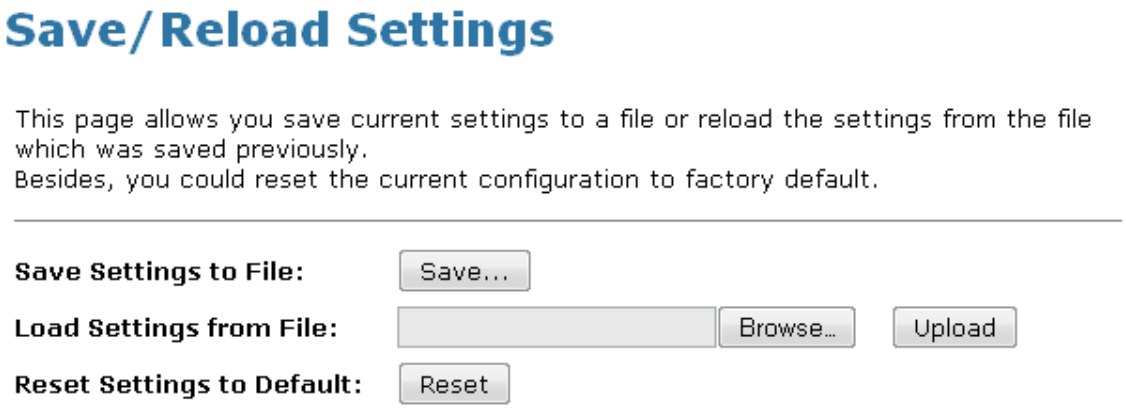
3. Se le modifiche apportate alla configurazione sono corrette, premere il pulsante Save e quindi individuare la cartella in cui salvare il file. Oppure premere Cancel per annullare


File Download
Do you want to save this file, or find a program online to open it?
Name: config.dat
Type: Unknown File Type, 3.99KB
From: 10.0.0.2
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

Lettura della configurazione da un file

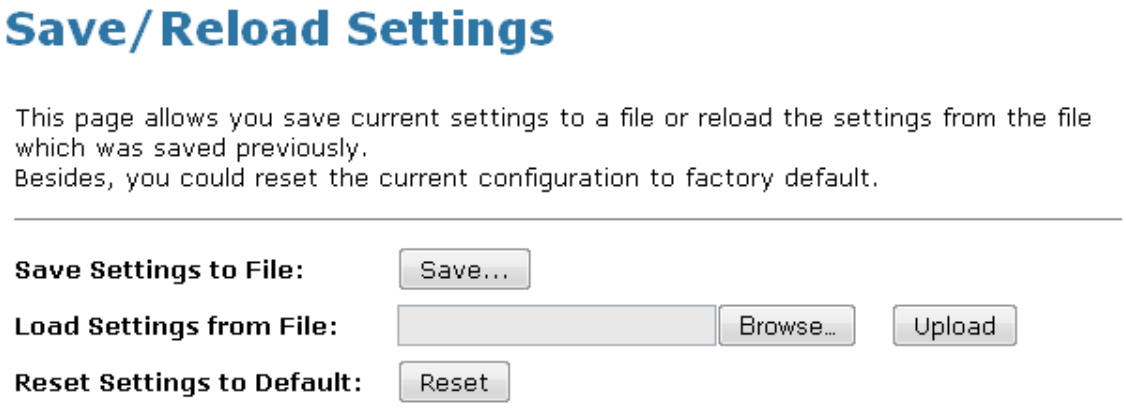
Tale operazione permette di rileggere i dati di configurazione da un file precedentemente salvato.

1. Dal menù di sinistra selezionare *Reset factory default*. Si visualizza la seguente pagina:

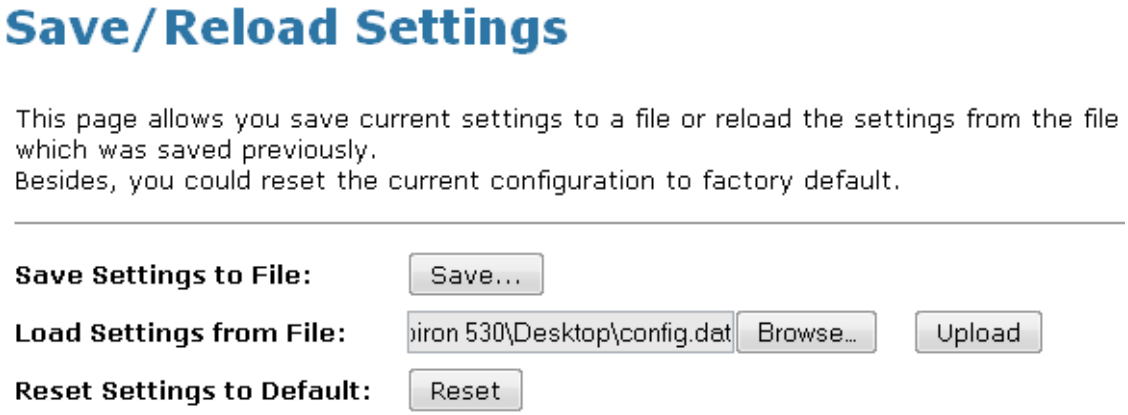

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

Schermata di Reset Factory default

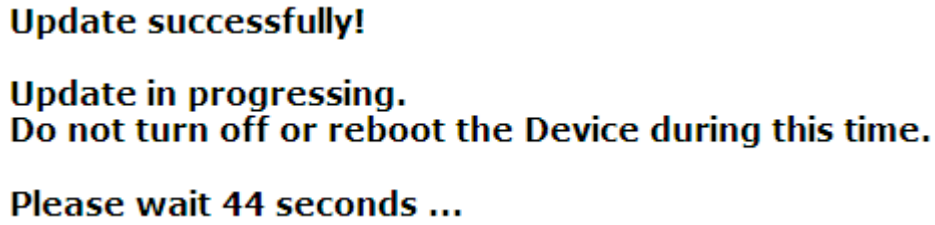
2. Premere *Browse*…. per individuare la cartella in cui è presente il file config.dat.


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

3. Dopo aver selezionato, per rileggere i dati premere *Upload*.


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
iron 530\Desktop\config.dat
Browse...
Upload
Reset Settings to Default:
Reset

4. Al termine della lettura dei dati dal file, si visualizzerà il seguente messaggio:
   Aggiornamento corretto!
   L'aggiornamento del dispositivo è in corso.
   Non spegnere o riavviare il dispositivo.
   Attendere 44 secondi ...



Ripristino dei valori di default

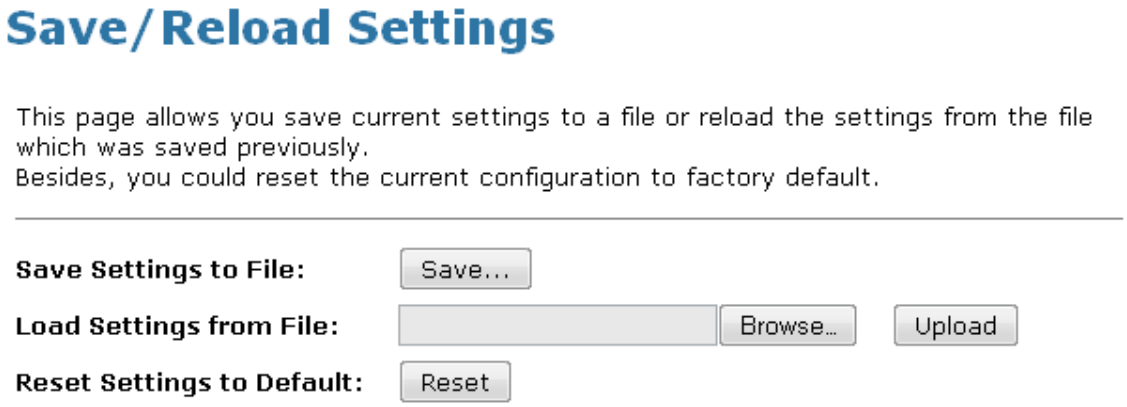
Qualora si siano effettuate modifiche alla configurazione e si voghlia ritornare alla configurazione iniziale del dispositivo, questo può essere fatto ripristinando i valori di default impostati in fabbrica.

Nota

Ripristinando i valori di fabbrica, tutte le modifiche apportate alla configurazione saranno perse e ripristinate dai valori di default.

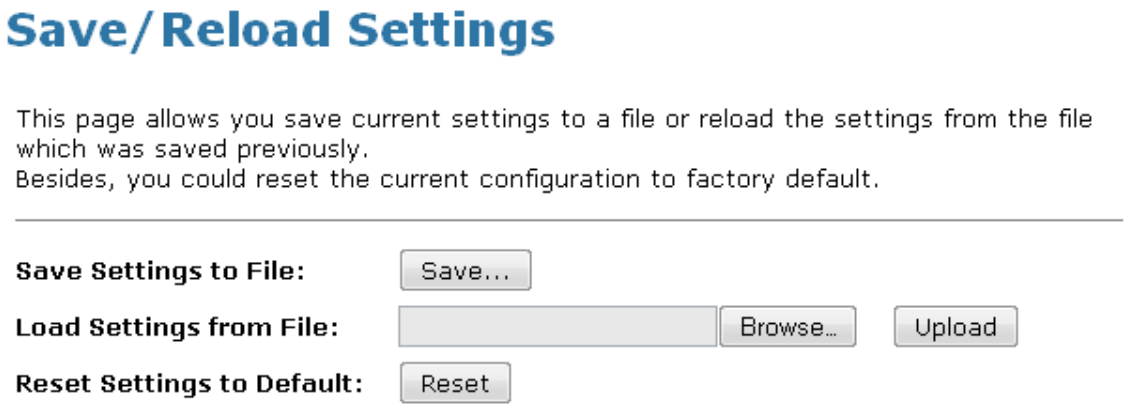
Reset software:

1. Dal menù di sinistra selezionare *Reset factory default*. Si visualizza la seguente pagina:

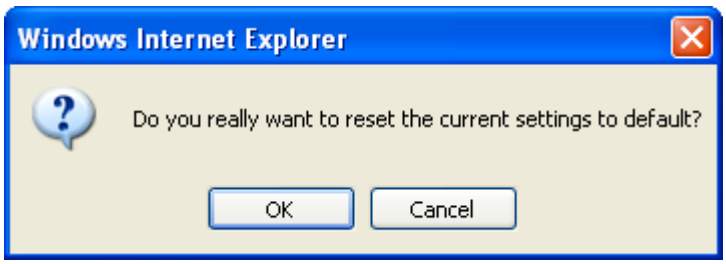

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

Schermata di Reset Factory default

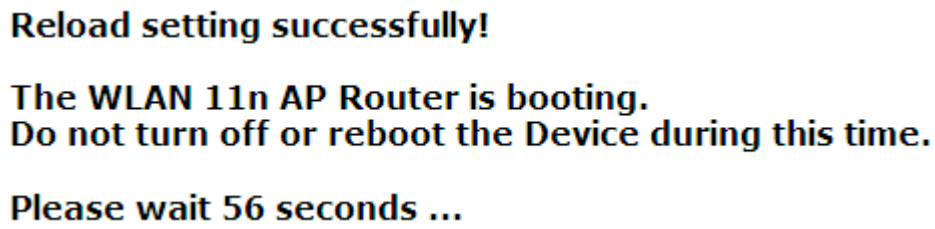
2. Premere il pulsante *Reset*, posto vicino all'opzione *Reset Settings to Default*.


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

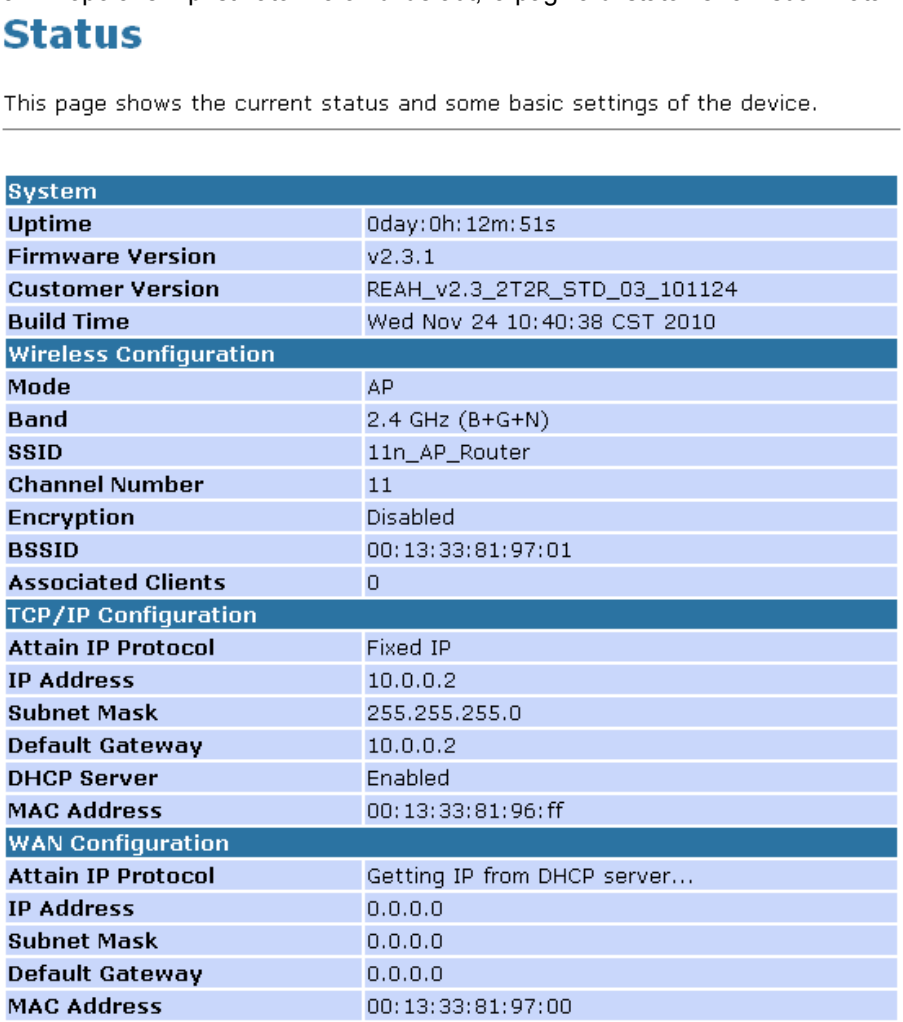
3. La pagina visualizzata ricorda che ripristinando i valori di fabbrica, tutte le modifiche apportate alla configurazione saranno irrimediabilmente cancellate, ripristinando tutte le configurazioni ai valori iniziali. L'operazione non potrà essere annullata. Per confermare, premere *OK*. Oppure premere *Cancel* per annullare



4. Si visualizza il seguente messaggio:
   Lettura completata correttamente!
   Attendere che il dispositivo si riavvia.
   Non spegnere o riavviare il dispositivo.
   Attendere 56 secondi ...


Reload setting successfully!
The WLAN 11n AP Router is booting.
Do not turn off or reboot the Device during this time.
Please wait 56 seconds ...

5. Dopo aver ripristinato i valori di defaut, la pagina di stato verrà visualizzata.



29 Password

Per aumentare la sicurezza del dispositivo è prevista una funzione di accesso protetto alle pagine WEB, mediante autenticazione a mezzo password. Con tale funzione abilitata, per accedere alle pagine di configurazione l'utente deve digitare il proprio Username e la relativa Password.

Di default, l'accesso autenticato mediante password è abilitato e la Username e Password sono preimpostate come segue:

Username: **admin**

Password: **hamlet**

Configurazione di Username e Password

Nota

Utenti non autorizzati potrebbero utilizzare la password di accesso per accedere al sistema. Si consiglia quindi di creare un nuovo Username ed una nuova Password quanto prima.

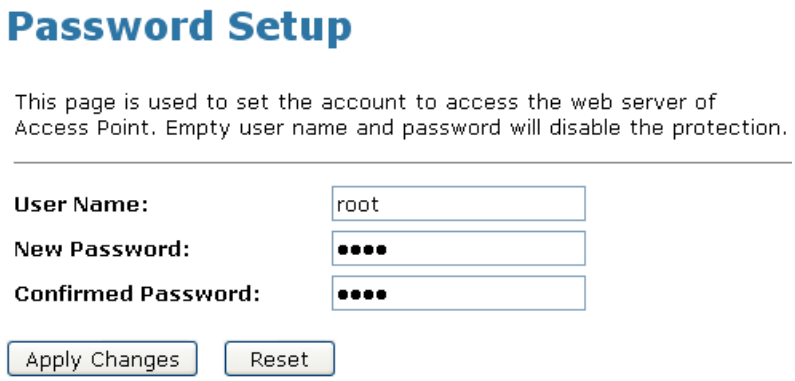
Per cambiare la password di default:

1. Dal menù di sinistra, selezionare Password. Si visualizza la seguente pagina:

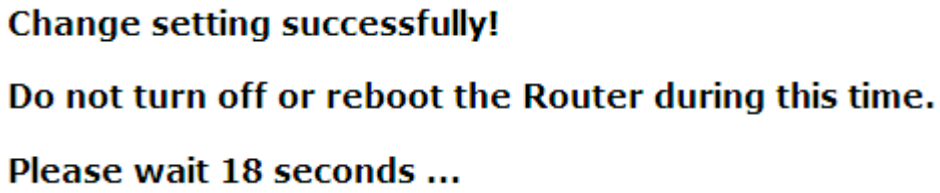
Password Setup
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.
User Name:
New Password:
Confirmed Password:
Apply Changes
Reset

2. Nella pagina sono visualizzate lo Username e la Password attualmente impostati. Digitare il nuovo Username e la nuova Password nei relativi Campi. La password deve essere digitata due volte al fine di assicurarsi di averla scritta correttamente. La password può essere una qualsiasi combinazione di lettere e numeri con lunghezza massima di 30 caratteri. Il default è predisposto con lo Username **admin** e la Password **hamlet**.

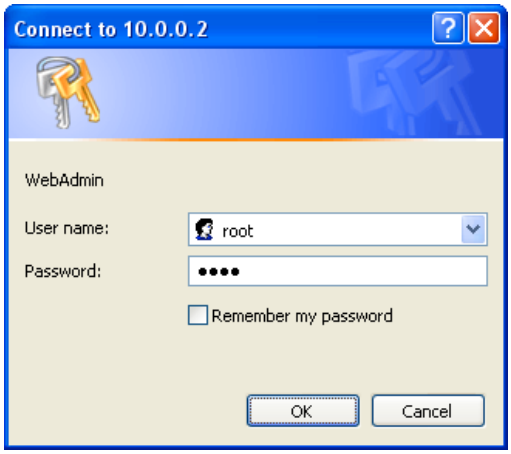
3. Dopo aver modificato i valori, confermare con il pulsante **Apply**. Nella pagina successiva, il nuovo utente viene visualizzato nella lista Currently Defined Users. Per effettuare il successivo login al sistema utilizzare il nuovo Username e la nuova Password.


Password Setup
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.
User Name:
root
New Password:
Confirmed Password:
Apply Changes
Reset

4. Si visualizza il seguente messaggio:
   Modifiche apportate correttamente.
   Non spegnere o riavviare il dispositivo.
   Attendere 18 secondi ...



5. Dalla pagina di Login, digitare il nuovo *Username* e la *Password*.
6. Premere *Apply*.



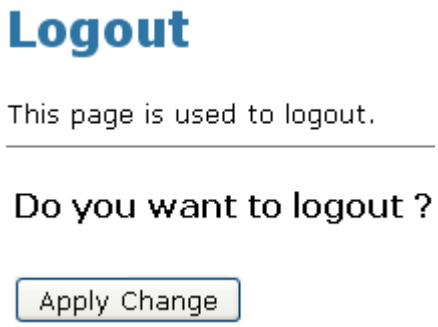
30 Logout

Questa pagina permette di effettuare il Logout.

Logout

Per effettuare il Logout::

1. Dal menù di sinistra, selezionare *Logout*. Si visualizza la seguente pagina:
2. Selezionare *Apply Change*.



A Configurazione dei Computer

La presente appendice fornisce le istruzioni per configurare la connessione Internet sul computer, così che possa interfacciarsi al Router AP.

Configurazione della connessione Ethernet sul PC

Prima di iniziare

Di default, il Router assegna automaticamente tutti i parametri operativi necessari per utilizzare Internet dai PC. E' quindi necessario configurare ciascun PC affinché riceva tutte le informazioni di configurazione automaticamente dal Router.

Nota

In alcuni casi, è possibile che si voglia configurare Internet manualmente (r alcuni PC o per tutti quelli connessi) anziché lasciarlo fare automaticamente dal Router. Si vedano le istruzioni per la “Assegnazione statica degli indirizzi IP sui computer".

- Se si è collegato il PC al Router mediante rete LAN Ethernet, si faccia riferimento a quanto descritto di seguito in funzione del sistema operativo installato sul PC:
- Windows® XP
- Windows 2000
- Windows Me
- Windows 95, 98

Windows® XP

1. Dalla barra dei comandi di Windows premere il pulsante *Start* e quindi selezionare il *Pannello di Controllo*.
2. Fare un doppio click su *Network Connections*
3. Nella finestra *LAN o High-Speed Internet*, fare click con il tasto destro del mouse sull'icona corrispondente alla scheda di rete (NIC . Network Interface Card) del PC e selezionare la voce *Proprietà*. Tipicamente tale icona è denominata *Local Area Connection* (*Connessione Rete Locale*).

La finestra delle proprietà della Connessione alla Rete Locale contiene l’elenco dei componenti di rete installati.

4. Assicurarsi che la voce *Internet Protocol TCP/IP* sia selezionata e quindi premere *Proprietà*.
5. Nella pagina delle proprietà del protocollo Internet (TCP/IP), selezionare *Obtain an IP address automatically* (*Ottieni un indirizzo IP automaticamente*). Selezionare anche l'opzione *Obtain DNS server address automatically* (*Ottieni l'indirizzo del Server DSN automaticamente*).
6. Premere due volte il pulsante *OK* per confermare le selezioni effettuate e quindi chiudere il Pannello di controllo.

Windows 2000

In prima fase, verificare se è presente il Protocollo IP e, in caso contrario, installarlo:

1. Dalla barra dei comandi di Windows premere il pulsante *Start* e quindi selezionare *Pannello di Controllo*.
2. Fare un doppio click su *Network Connections* (*Connessioni di Rete*) e quindi su *Dial-Up*.
3. Nella finestra *Network and Dial-up Connections*, fare click con il tasto destro del mouse sull'icona *Local Area Connection* (*Connessione Area Locale*) e selezionare la voce *Proprietà*.

La finestra delle proprietà contiene un elenco dei componenti di rete installati. Se nella lista è gia presente la voce *Internet Protocol (TCP/IP)*, il protocollo IP è già installato ed abilitato. Andare al passo 10.

4. Se la voce *Internet Protocol (TCP/IP)* non è visualizzata tra i componenti installati, premere il pulsante *Install…*
5. Nella finestra *Select Network Component Type*, selezionare *Protocol* e quindi premere il pulsante *Add…*
6. Selezionare *Internet Protocol (TCP/IP)* dall'elenco *Network Protocols* (protocolli di rete) e quindi premere *OK*.

Potrebbe essere richiesto di utilizzare il CD di installazione di Windows 2000 (o altro dispositivo da cui si è effettuata l'installazione) per installare correttamente il driver. Seguire le istruzioni visualizzate per installare il protocollo TCP/IP.

7. Quando richiesto, premere *OK* per riavviare il computer e rendere operative le nuove configurazioni.

Successivamente, configurare il computer per farsi assegnare gli indirizzi IP dal Router:

8. Dal Pannello di Controllo, premere due volte l'icona *Network and Dial-up Connections*.
9. Nella finestra *Network and Dial-up Connections*, fare click con il tasto destro del mouse sull'icona *Local Area Connection* e selezionare la voce Proprietà.
10. Nella finestra delle proprietà, selezionare *Internet Protocol (TCP/IP)* e quindi premere il pulsante Proprietà.
11. Nella pagina delle proprieta del Protocollo Internet (TCP/IP), selezionare *Obtain an IP address automatically*. Selezionare anche l'opzione *Obtain DNS server address automatically*.
12. Premere due volte *OK* per confermare e salvare i cambiamenti apportati e quindi chiudere il Pannello di Controllo.

Windows Me

1. Dalla barra dei comandi di Windows premere il pulsante *Start* e quindi selezionare *Settings* e quindi *Pannello di Controllo*.
2. Fare un doppio click sull'icona *Network and Dial-up Connections*.
3. Nella finestra *Network and Dial-up Connections*, fare click con il tasto destro del mouse sull'icona *Network* (Rete) e selezionare la voce Proprietà.

La finestra delle proprietà contiene un elenco dei componenti di rete installati. Se nella lista è gia presente la voce *Internet Protocol (TCP/IP)*, il protocollo IP è già installato ed abilitato. Andare al passo 11.

4. Se la voce *Internet Protocol (TCP/IP)* non è visualizzata tra i componenti installati, premere il pulsante *Add…*
5. Nella finestra *Select Network Component Type*, selezionare *Protocol* e quindi premere il pulsante *Add…*
6. Selezionare *Microsoft* nell'elenco dei Costruttori (Manufacturer).
7. Selezionare *Internet Protocol (TCP/IP)* dall'elenco *Network Protocols* (protocolli di rete) e quindi premere *OK*.

Potrebbe essere richiesto di utilizzare il CD di installazione di Windows ME (o altro dispositivo da cui si è effettuata l'installazione) per installare corettamente il driver. Seguire le istruzioni visualizzate per installare il protocollo TCP/IP.

8. Quando richiesto, premere *OK* per riavviare il computer e rendere operative le nuove configurazioni.

Successivamente, configurare il computer per farsi assegnare gli indirizzi IP dal Router:

9. Dal Pannello di Controllo, premere due volte sulla icona *Network and Dial-up Connections*.
10. Nella finestra *Network and Dial-up Connections*, fare click con il tasto destro del mouse sull'icona *Network* (Rete) e selezionare la voce Proprietà.
11. Nella finestra delle proprietà, selezionare *TCP/IP* e quindi premere il pulsante Proprietà.

12. Nella pagina delle proprieta del protocollo TCP/IP, selezionare l'opzione *Server assigned IP address* (Indirizzo IP assegnato dal Server). Selezionare anche l'opzione *Server assigned name server address*.
13. Premere due volte *OK* per confermare e salvare i cambiamenti apportati e quindi chiudere il Pannello di Controllo.

Windows 95, 98

In prima fase, verificare se è presente il Protocollo IP e, in caso contrario, installarlo:

1. Dalla barra dei comandi di Windows premere il pulsante *Start*, selezionare *Settings* e quindi selezionare *Pannello di Controllo*.
2. Fare un doppio click sull'icona *Network* (Rete).

La finestra *Network* (connessioni di rete) contiene l'elenco dei componenti di rete installati. Se nella lista è gia presente la voce TCP/IP, il protocollo IP è già installato ed abilitato. Andare al passo 9.

3. Se la voce TCP/IP non è visualizzata tra i componenti installati, premere il pulsante *Add...*

Verrà visualizzata la finestra *Select Network Component Type*.

4. Selezionare *Protocol* e quindi premere il pulsante *Add…*

Verrà visualizzata la finestra relativa.

5. Selezionare *Microsoft* nell'elenco dei costruttori (Manufacturers) e quindi selezionare *TCP/IP* nell'elenco dei protocolli.
6. Premere *OK* per tornare alla finestra della connessione di rete e quindi premere nuovamente *OK*.

Potrebbe essere richiesto di utilizzare il CD di installazione di Windows 95/98 per installare corettamente il driver. Seguire le istruzioni visualizzate per installare il protocollo TCP/IP.

7. Premere *OK* per riavviare il PC e completare l'installazione del protocollo TCP/IP.

Successivamente, configurare il computer per farsi assegnare gli indirizzi IP dal Router:

8. Aprire la finestra del Pannello di Controllo e selezionare l'icona *Network*.
9. Selezionare il componente denominato *TCP/IP* e quindi premere *Proprietà*.

Se nella lista sono presenti più componenti TCP/IP, selezionare quello relativo alla scheda di rete.

10. Nella pagina delle proprieta del Protocollo Internet (TCP/IP), premere il tab dell'indirizzo IP (IP Addrress).
11. Selezionare anche l'opzione *Obtain an IP address automatically*.
12. Premere il tab Configurazione DNS e quindi selezionare l'opzione *Obtain an IP address automatically*.
13. Premere due volte *OK* per confermare e salvare i cambiamenti apportati.

Verrà richiesto di riavviare Widows.

14. Premere SI.

Assegnazione statica degli indirizzi IP sui computer

Se non si hanno esigenze particolari, non è necessario assegnare le informazioni per l'accesso ad Internet in modo statico, poichè tali informazioni sono assegnate automaticamente dal vostro ISP.

Tuttavia, in alcuni casi, si può voler assegnare tali informazioni in modo statico a tutti o solo alcuni PC, anzichè permettere l'assegnazione automatica dal router. Questa opzione può essere applicabile (ma non necessaria) se:

- si è in possesso di uno o più indirizzi IP pubblici che si vogliono associare a specifici computer (ad esempio, qualora si utilizzi un computer come Web Server pubblico).
- Si utilizzino differenti sottoreti sulla propria rete (le sottoreti sono descritte in Appendice B).

Prima di iniziare, è necessario disporre delle seguenti informazioni:

- L'indirizzo IP e la Subnet Mask di ciascun PC.
- L'indiizzo IP del Default Gateway della rete LAN. Nella maggior parte dei casi tali indirizzo è quello assegnato alla porta LAN del Router. Di default, alla porta LAN è assegnato l'indirizzo IP 10.0.0.2. (Si può cambiare questo indirizzo oppure un indirizzo differente può essere assegnato dal vostro ISP). Si veda il paragrafo 'Assegnazione degli indirizzi' per ulteriori informazioni)
- L'indirizzo IP del server DNS (Domain Name System) assegnato dal vostro ISP.

Su ciascun PC a cui assegnare gli indirizzi in modo statico, seguire le istruzioni relative alla sola verifica e/o installazione del protocollo IP. Dopo che questo è stato installato, seguire le istruzioni per visualizzare le proprietà del protocollo TCP/IP (Internet Protocol). Anziché abilitare l'assegnazione dinamica dell' indirizzo IP del computer, del server DNS e del Default Gateway, selezionare l'opzione per assegnare tali parametri in modo manuale.

Nota

L'indirizzo IP da assegnare al PC deve essere compreso nella sottorete a cui è collegata la porta LAN del Router. Se i parametri di indirizzamento IP sono assegnati manualmente, è necessario attenersi alle istruzioni fornite per cambiare l'indirizzo IP della porta LAN.

B Indirizzi IP, Network e Subnet Mask

Indirizzi IP

Nota

Questa sezione fa riferimento solamente agli indirizzi IP utilizzati nel protocollo IPv4 (versione 4 del Protocollo Internet). Gli indirizzi IP utilizzati nel protocollo IPv6 non sono compresi.

Per la lettura della presente appendice si assume che le conoscenze basi relative ai numeri binari, al concetto di bit e byte siano conosciuti.

Gli indirizzi IP sono la versione equivalente dei numeri telefonici da usarsi nelle comunicazioni Internet e servono per identificare univocamente i singoli nodi (computer o dispositivi di rete) sulla rete Internet. Ciascun indirizzo IP è composto di quattro valori numerici, ognuno dei quali può variare tra 0 e 255. Ciascun valore è separato dall'altro mediante un punto (ad esempio l'indirizzo IP 20.56.0.211). I quattro valori numerici sono chiamati, rispettivamente da sinistra a destra, campo1, campo2, campo3 e campo4.

La notazione per scrivere un indirizzo IP è definita come "notazione decimale puntata" (in inglese: dotted decimal notation). L'indirizzo IP 20.56.0.211 si legge come "venti punto cinquantasei punto zero punto duecentoundici".

Struttura di un indirizzo IP

Gli indirizzi IP hanno una struttura gerarchica simile a quella dei numeri telefonici. Ad esempio, un classico numero telefonico composto da 7 cifre inizia con un prefisso di 3 cifre che identifica un gruppo di migliaia di linee telefoniche, mentre le restanti quattro cifre identificano la linea telefonica specifica di quel gruppo.

Analogamente, l'indirizzo IP contiene due tipi di informazioni:

- *Network ID*
  Identifica una particolare rete contenuta nella rete globale Internet ovvero una rete Intranet
- *Host ID*
  Identifica uno specifico computer o dispositivo all'interno della rete

La prima parte di ciascun indirizzo IP contiene l'identificatore di rete (Network ID), mentre le restanti cifre identificano il computer (Host ID). La lunghezza del Network ID dipende dalla classe della rete (si veda la sezione seguente). La seguente tabella mostra la struttura di un indirizzo IP.

	Campo1	Campo2	Campo3	Campo4
Classe A	Network ID	Host ID		
Classe B	Network ID		Host ID	
Classe C	Network ID			Host ID

Di seguito si riportano alcuni esempi di indirizzi IP validi:

Classe A: 10.30.6.125 (network = 10, host = 30.6.125)
Classe B: 129.88.16.49 (network = 129.88, host = 16.49)
Classe C: 192.60.201.11 (network = 192.60.201, host = 11)

Classi di reti

Le tre classi più comunemente utilizzate sono definite come A, B e C (Esiste anche una Classe D ma è utilizzata per scopi specifici che esulano dalla presente descrizione). Queste classi hanno differenti usi e caratteristiche.

Le reti di Classe A sono le reti più estese, facenti parte della rete Internet. Ciascuna rete può contenere fino a 16 milioni di host (computer e/o dispositivi di rete). Possono esistere fino ad un massimo di 126 di queste reti, per un totale di oltre 2 miliardi di host. A causa delle enormi dimensioni, tali rete sono utilizzate come WAN dalle organizzazioni a livello di infrastruttura di Internet, quali ad esempio gli ISP (Internet Service Provider).

Le reti di Classe B sono più piccole ma comunque sempre estese, essendo ciascuna capace di gestire fino a oltre 65.000 host. Possono esistere fino ad un massimo di 16.384 reti in Classe B. Una rete in classe B potrebbe essere appropriata per organizzazione di grandi dimensioni quali le agenzie governative o per industrie di grandi dimensioni.

Le reti in Classe C sono le più piccole, capaci di gestire un massimo di 254 host; tuttavia il numero totale di reti in Classe C è superiore a 2 milioni (per l'esattezza 2.097.152). Le reti LAN collegate ad Internet sono normalmente reti di Classe C.

Alcue note importanti riguardanti gli indirizzi IP:

- La classe della rete può essere determinata facilmente dal valore del primo campo (Campo1):
  campo1 = 1-126: Classe A
  campo1 = 128-191: Classe B
  campo1 = 192-223: Classe C
  (Quando il valore del campo1 non è visualizzato, l'indirizzo è riservato per specifici usi)
- Un host ID può assumere qualsiasi valore ad eccezione di tutti i valori a 0 o tutti i valori a 255; tali indirizzi sono riservati per usi particolari.

Subnet mask

Definizione
mask

Una Mask si compone come un normale indirizzo IP, ma si utilizza per definire una maschera di bit che identifica quale parte dell'indirizzo IP deve essere considerato come network ID e quale parte come host ID: i bit impostati a 1 indicano che il bit in quella posizione è parte della "network ID", mentre i bit impostati a 0 indicano che il bit in quella posizione è parte dell' "host ID".

Le Subnet Mask sono utilizzate per definire delle sottoreti (che si ottengono per dividere una rete in parti più piccole). Un Network ID di una sottorete si crea prendendo "in prestito" uno o più bit della porzione relativa all'host ID. La Subnet mask ha quindi il compito di identificare tali bit.

Per esempio, si consideri una rete di Classe C definita come 192.168.1. Per dividere questa rete in due sottoreti, si può utilizzare la subnet mask:

255.255.255.128

E' facile vedere la differenza riscrivendo il valore in codice binario:

11111111. 11111111. 11111111.10000000

Gli indirizzi di reti in Classe C, tutti i bit dei campi da field1 a field3 sono parti del Network ID, ma si noti che la Subnet Mask specifica che il primo bit del quarto valore deve essere compreso nella Network ID. Poichè tale bit extra può assumere solo due valori (0 ed 1), ciò significa che esisteranno due sottoreti. Ciascuna sottorete utilizzerà i rimante 7 bit del field4 per assegnare l'Host ID, con un range di Host compreso tra 1 e 126 (in sostituzione del normale range di indirizzi in Classe C compresi tra 0 e 255).

Analogamente, volendo dividere una rete in Classe C in 4 sottoreti, la Subnet Mask sarà:

255.255.255.192
o
11111111. 11111111. 11111111.11000000

I due bit del campo4 possono assumere 4 valori (00, 01, 10, 11), così da creare quattro sottoreti. Ciascuna sottorete potrà utilizzare i restanti 6 bit del field4 per identificare i propri host IDs, nel range da 1 a 62.

Nota

Talvolta una subnet mask non specifica alcun bit extra e quindi nessuna sottorete. In questo caso si definisce come Subnet Mask di default. Tali Subnet Mask sono:

Classe A: 255.0.0.0
Classe B: 255.255.0.0
Classe C: 255.255.255.0

Tali Subnet Mask sono chiamate di default poichè si utilizzano quando la rete è configurata inizialmente per non avere sottoreti.

C UPnP Control Point Software su Windows ME/XP

La presente appendice fornisce le istruzioni per configurare la UPnP sul computer per operare con il Router AP.

L' UPnP è una architettura per permettere la connessione peer-to-peer di apparati intelligenti, dispositivi Wireless e computer di qualsiasi tipo. E' progettato per permettere una connettività facile, flessibile e basata su un metodo standard, in reti di tipo 'non gestite' quali possono essere le reti nelle abitazioni, in piccole aziende, in spazi pubblici o connessioni ad Internet. UPnP è una architettura aperta e distribuita che si appoggia al protocollo TCP/IP ed alle tecnologie Web per abilitare l'accesso a reti senza gestore e permettere lo scambio dati tra dispositivi presenti in casa, ufficio o spazi pubblici.

UPnP è più di una semplice estensione del modello di 'periferiche plug and play'. E' progettata per avere caratteristiche quali zero-configuration, rete "invisibile" e rilevamento automatico di un ampia gamma di categorie di dispositivi di vari costruttori. Ciò significa che un dispositivo può dinamicamente unirsi ad una rete, ottenere un indirizzo IP, condividere le proprie risorse e rilevare ed utilizzare le risorse dei dispositivi già presenti nella rete. Server DHCP e DNS sono opzionali e sono utilizzati solo se presenti. Infine, un dispositivo può lasciare la rete in modo automatico senza che rimangano connessioni appese.

UPnP Control Point Software su Windows ME

Per installare il software UPnP Control Point su Windows ME:

1. Dal Pannello di Controllo selezionare "Add/Remove Programs" ("Aggiungi/Rimuovi Applicazioni").
2. Nella finestra delle proprietà selezionare il tab "Windows Setup" e nell'elenco dei "Componenti", fare doppio click su "Communications".
3. Nella finestra "Communications", scorrere la lista "Components" per selezionare la voce UPnP. Selezionare tale voce e premere "OK".
4. Premere "OK" per completare l'operazione.
5. Riavviare il sistema.

Dopo aver installato il software UPnP ed aver riavviato il sistema (e la rete include il sistema IGD - Internet Gateway Device), si dovrebbe poter vedere il dispositivo IGD sulla rete.

UPnP Control Point Software su Windows XP con Firewall

Sulle versioni di Windows XP precedenti al Service Pack 2, il supporto Firewall è dato dal componente *Windows XP Internet Connection Firewall*. Tale componente non può essere utilizzato su sistemi con il controllo UPnP. Pertanto, se tale firewall è attivo, il sistema di controllo non potrà visualizzare l'elenco dei dispositivi associati e quindi non potrà comunicare in modalità UPnP (Questa restrizione si applica anche ai dispositivi controllati basati su sistemi Windows XP precedenti alla SP2).

Sui sistemi Windows XP SP2 o superiori, la funzione di firewall la realizza il componente *Windows Firewall*. Diversamente dalle precedenti versioni, Windows XP SP2 può essere utilizzato su sistemi che si vogliano impiegare come punti di controllo dell' UPnP.

Per disattivare il Firewall in qualsiasi versione di Windows XP, attenersi alle seguenti istruzioni:

1. Dal Pannello di Controllo selezionare "Network and Internet Connections".
2. Dalla relativa schermata selezionare "Network Connections".
3. Nella finestra delle connessioni di rete, fare click con il tasto destro del mouse sull'icona Connessione Area Locale (Local Area Connection), visualizzando il menù relativo. Selezionare la voce "Proprietà".
4. Nella finestra delle proprietà selezionare il tab "Advanced". Disabilitare il Firewall sulla connessione, deselezionando la seguente voce:

"Protect my computer and network by limiting or preventing access to the computer from the Internet"
(Proteggi il computer e la rete limitando o impedendo l'accesso al computer da Internet)

5. Premere "OK".

Requisiti SSDP

Per utilizzare il software UPnP deve essere abilitato il servizio di Windows XP *SSDP Discovery Service*.

Tale servizio è abilitato di default durante l'installazione di Windows XP. Per verificare che il servizio è abilitato sul proprio computer, cercare in *Control Panel* > *Administrative Tools* > *Services*.

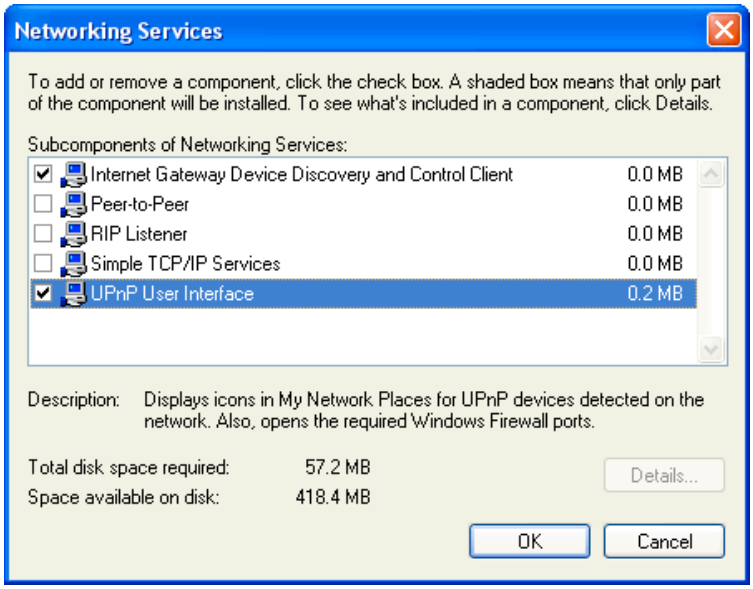
Procedura di installazione

Per installare il software UPnP Control Point su Windows XP, attenersi a quanto segue:

1. Dal Pannello di Controllo selezionare "Add/Remove Programs" (Aggiungi/Rimuovi Applicazioni).
2. Dalla finestra visualizzata, premere il pulsante "Add / Remove Windows Components" (Aggiungi / Rimuovi Componenti Windows).
3. Nel Wizard che viene visualizzato, scorrere l'elenco dei "Servizi di Rete". Evidenziare (selezionare) la voce e premere il pulsante "Dettagli".
4. Si visualizza la finestra dei Servizi di Rete.

I componenti elencati in tale finestra saranno differenti in funzione della versione Windows XP che si sta utilizzando: Windows XP, Windows XP (SP1), or Windows XP (SP2).

Se si sta utilizzando Windows XP SP2, i Servizi di Rete visualizzati conterranno i seguenti componenti:


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.
Total disk space required: 57.2 MB
Space available on disk: 418.4 MB
Details...
OK
Cancel

5. Selezionare le seguenti voci dall'elenco dei "Servizi di Rete" e quindi premere "OK":

Se si utilizza **Windows XP**, selezionare:

• "Universal Plug and Play".

Se si utilizza **Windows XP SP1**, selezionare:

• "Internet Gateway Device discovery and Control Client".

• "Universal Plug and Play".

Se si utilizza **Windows XP SP2**, selezionare:

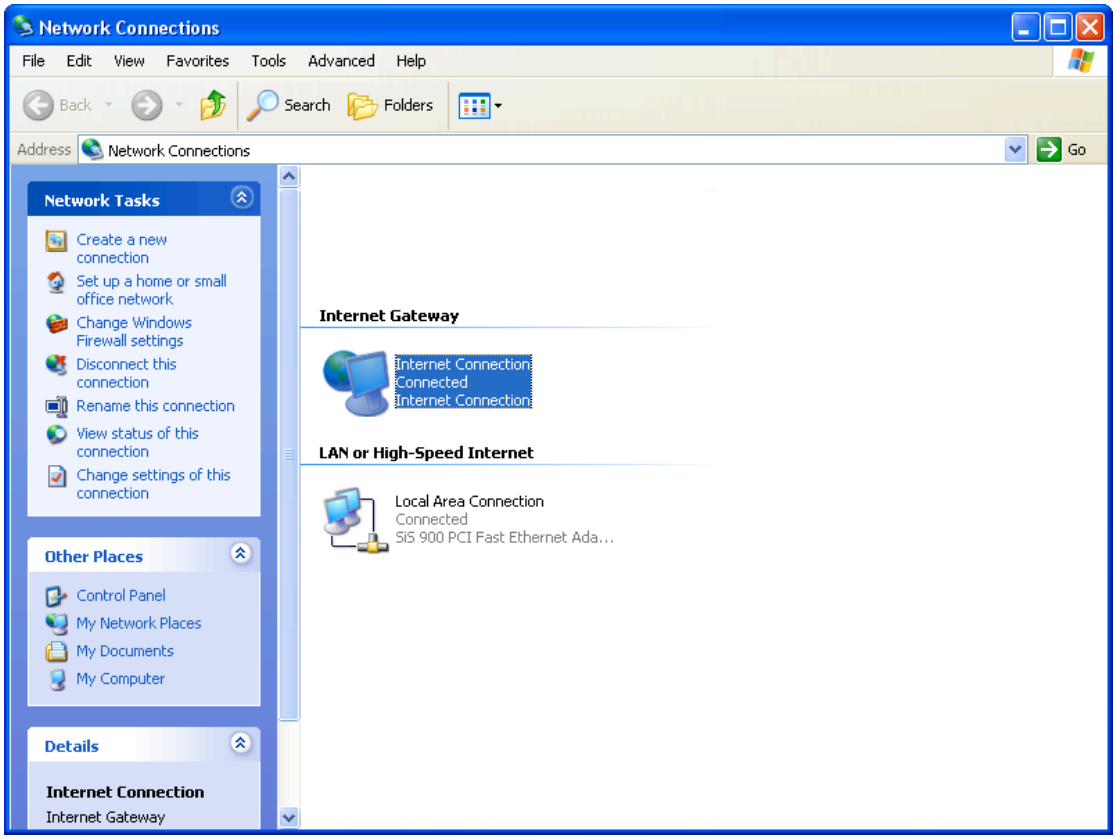
• "Internet Gateway Device discovery and Control Client".

• "UPnP User Interface".

6. Riavviare il sistema.

Dopo aver installato il software UPnP ed aver riavviato il sistema (e la rete include il sistema IGD - Internet Gateway Device), si dovrebbe poter vedere il dispositivo IGD sulla rete.

Per esempio, dalla finestra delle connessioni di rete si potrebbe vedere Il dispositivo “Internet Gateway”:



D Risoluzione dei problemi

La presente appendice elenca le possibili soluzioni che possono essere applicate qualora si riscontrino problemi in fase di installazione o utilizzo del Router. Fornisce inoltre le istruzioni per utilizzare utility di diagnostica per le funzionalità di connessione in rete IP.

Contattare il Supporto Tecnico del fornitore qualora non si riesca a risolvere il problema attenendosi a quanto di seguito descritto.

Suggerimenti per la soluzione dei problemi

Anomalia	Ricerca del guasto
LED	
Il LED Power non si illumina quando l'apparato è acceso.	Verificare che si sta utilizzando il cavo di alimentazione e l'adattatore fornito con il dispositivo e che sia correttamente collegato sia al Router che alla presa a muro.
Il LED LAN non si accende quando il cavo Ethernet è collegato.	Assicurarsi che il cavo di rete Ethernet sia correttamente collegato sia all'HUB della LAN o al PC sia al Router. Assicurarsi che il PC e/o l'HUB siano accesi. Verificare che il cavo utilizzato sia idoneo ai requisiti della rete in uso. Una rete a 100 Mbit/sec (10BaseTx) dovrebbe utilizzare cavi con etichetta CAT 5. Una rete a 10Mbit/sec può funzionare anche con cavi di qualità inferiore.
Connessione Internet	
Il PC non riesce ad accedere a Internet	Utilizzare l'utility PING (descritta di seguito nella presente sezione) per verificare se il PC riesce a comunicare con il dispositivo della LAN, identificandoll mediante il relativo indirizzo IP (di default 10.0.0.2). Se non si riesce a comunicare, verificare il cavo Ethernet. Se si è assegnato un indirizzo IP statico al computer, (non un indirizzo pubblico registrato), verificare quanto di seguito: • controllare che l'indirizzo IP del Gateway sul computer sia l'indirizzo IP pubblico (si veda il paragrafo Stato per le istruzioni necessarie a vedere gli indirizzi IP). Se non è corretto, modificare il valore dell'indirizzo IP oppure predisporre il PC per ricevere gli indirizzi in modo automatico. • Verificare con l'ISP che il Server DNS specificato sul PC sia corretto. In caso corregge l'indirizzo oppure predisporre il PC per riceverlo automaticamente.
I PC connessi su LAN non riescono a visualizzare le pagine WEB su Intenet.	Verificare che l'indirizzo IP del Server DNS specificato sul PC sia corretto che i valori forniti dall'ISP, come descritto nel passo precedente. Se si è specificato di ricevere i dati del Server DNS in modo dinamico, assicurarsi che i valori impostati sul Router corrispondano con quelli forniti dall' ISP. Ulteriormente è possibile utilizzare l'utility PING per verificare la connessione con il Server DNS dell' ISP.
Pagine Web	
Si è persa la User ID o la password.	Se non si sono modificati i valori di default, provare ad utilizzare lo User ID "admin" e la password "hamlet". In alternativa, è possibile ripristinare il dispositivo alla configurazione di default, premendo il pulsante Reset Default posto sul pannello posteriore del dispositivo. Quindi, ridigitare lo User ID e la Password di default, mostrati di seguito. **ATTENZIONE:** Resettando il dispositivo ai valori di default, si perdono tutte le modifiche apportate alla configurazione, ripristinando i valori di fabbrica.

Anomalia	Ricerca del guasto
Non è possibile accedere alle pagine web dal browser.	Utilizzare l'utility PING, come descritto in precedenza, per verificare che il PC riesca a comunicare con l'indirizzo IP della porta LAN del dispositivo (di default 10.0.0.2). Se non si riesce a comunicare, verificare il cavo Ethernet. Verificare che si stla utilizzando un browser tipo Internet Explorer o Netscape Navigator v4.0 o superiore. Verificare che l'indirizzo IP del PC sia definito nella stessa sottorete su cui è assegnato l'indirizzo IP della porta LAN del dispositivo..
Le modifiche apportate alle pagine Web non vengono salvate.	Assicurarsi di aver premuto il pulsante *Confirm Changes/Apply* dopo ogni cambiamento.

Diagnostica mediante le utility IP

ping

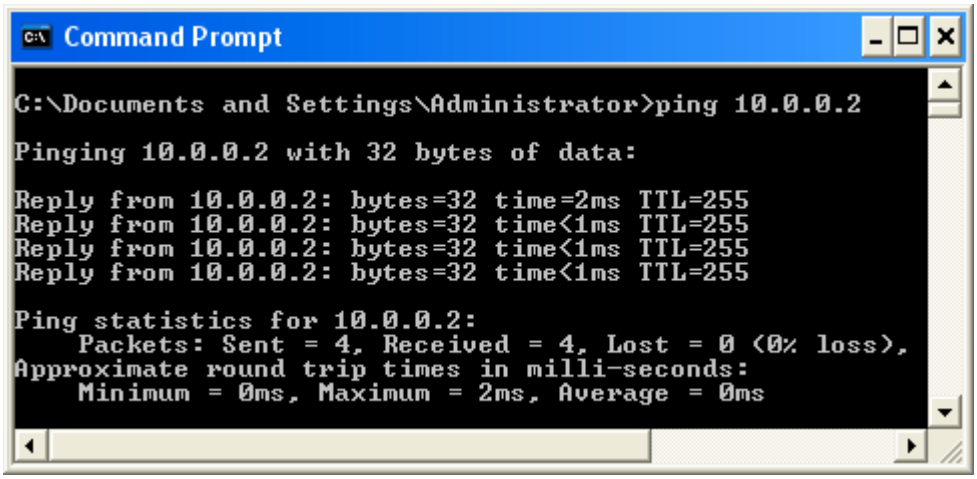
Il comando *PING* consente di verificare se il computer è in grado di comunicare con un altro computer sulla rete ed Internet. Il comando di PING invia un messaggio al computer specificato nel comando. Se il computer riceve il comando, invia un messaggio di risposta. Per utilizzare questa utility, si deve conoscere l'indirizzo IP del computer con cui si vuole comunicare.

Sui computer con sistema operativo Windows, si può eseguire un comando di PING dal menù Start. Premere il pulsante *Start* e quindi selezionare *Run* (Esegui). Nella finestra che si apre, digitare il seguente comando:

ping 10.0.0.2

Premere *OK*. Si può sostituire l'indirizzo IP con un qualsiasi indirizzo della rete LAN (indirizzo privato) o con un indirizzo IP pubblico di un sito Internet (se lo si conosce).

Se il computer interrogato riceve il messaggio inviato, si apre una Shell dei Comandi:


Command Prompt
C:\Documents and Settings\Administrator>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=2ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms

Se il computer interrogato non può essere localizzato, verrà visualizzato un messaggio di TimeOut (*Request timed out*).

Utilizzando l'utility PING è possibile verificare se l'intero percorso di collegamento al Router (identificato dall'indirizzo IP della Porta LAN 10.0.0.2) o un altro indirizzo della rete funziona correttamente.

E' possibile inoltre verificare l'accesso ad Internet digitando un indirizzo IP esterno, quale ad esempio l'indirizzo di sito *www.yahoo.com* (216.115.108.243). Se non si conosce l'indirizzo IP di una particolare posizione Internet, si può far ricorso all'utility *nslookup*, come descritto nel successivo paragrafo.

Gli stessi comandi sono disponibili in vari sistemi operativi in cui si utilizza il protocollo IP, avviandoli al prompt dei comandi ovvero mediante utility di Amministrazione del Sistema.

nslookup

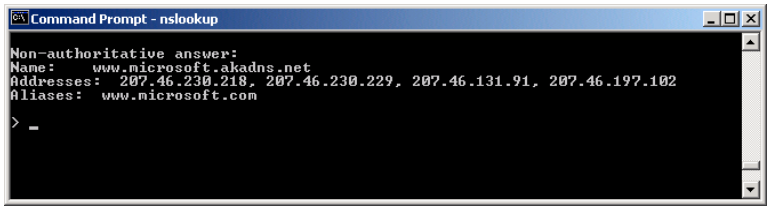
E' possibile utilizzare il comando nslookup per determinare l'indirizzo IP di un sito Internet a partire dal nome del dominio. Specificando il nome del dominio, il comando nslookup cerca il nome all'interno del Server DNS (normalmente localizzato con l'ISP). Se il nome non è presente nella tabella DNS dell' ISP, la richiesta è reinviata ad un Server di livello più alto e così via finché non viene trovato il valore cercato. Al termine della ricerca, il server ritorna l'indirizzo IP associato.

Sui computer basati su sistema operativo Windows, è possibile eseguire il comando nslookup dal menù Start. Premere il pulsante *Start* e quindi selezionare *Run* (Esegui). Nella finestra che si apre, digitare il seguente comando:

Nslookup

Premere *OK*. Si visualizza la schermata dei Prompt dei Comandi, con il simbolo ">" come prompt. Digitare l'indirizzo Internet di cui si vuole conoscere l'indirizzo IP, come ad esempio *www.microsoft.com*.

In risposta, verrà visualizzato l'indirizzo IP associato (se conosciuto) come mostrato di seguito:



Possono esserci diversi indirizzi IP associati allo stesso indirizzo Internet. Questo si verifica tipicamente per siti con ungrande traffico dati, per cui utilizzano più Server in ridondanza per gestire le stesse informazioni.

Per terminare l'utility nslookup, digitare **exit** (e premere **Invio**) al prompt dei comandi.

E Glossario

10BASE-T

Il tipo di interfaccia alla rete Ethernet standard impiegata in reti locali con velocità fino a 10 Mbps. I cavi utilizzati sono denominati Categoria 3 (CAT 3). Si veda *data rate, Ethernet*.

100BASE-T

Il tipo di interfaccia alla rete Ethernet standard impiegata in reti locali con velocità fino a 100 Mbps. I cavi utilizzati sono denominati Categoria 5 (CAT 5). Si veda *data rate, Ethernet*.

ADSL

Asymmetric Digital Subscriber Line
IL DSL asimmetrico è l'utilizzo più comune della tecnica DSL per gli utenti di tipo "home". Il termine asimmetrico si riferisce alla differenza di velocità tra "download" ed "upload" (normalmente la velocità di download è superiore quella di upload). Tale condizione diventa un beneficio per gli utenti residenziali, in quanto tipicamente utilizzano Internet maggiormente per operazioni di download dei dati che non per upload.

Analogico

Un segnale analogico è un segnale può variare la propria frequenza in vari modi, quale ad esempio per amplificazione dell'intensità o variando il valore di frequenza, allo scopo di aggiungere informazioni sul segnale. La componene "voce" in DSL è un segnale analogico. Si veda *Digitale*.

ATM

Asynchronous Transfer Mode
E' un standard per trasmissioni ad alta velocità di dati, testo, voce e video, largamente utilizzata in Internet. Il range dei dati in ATM varia tra 45 Mbps a 2.5 Gbps. Si veda *data rate*.

Autenticazione

L'autenticazione permette di identificare un utente, mediante l'utilizzo di password.

Binario

E' un sistema numerico, in base "due" che utilizza solamente due valori (0 ed 1) per rappresentare tutti i numeri. In binario, il numero 1 si scrive come 1, il 2 come 10, il 3 come 11, il 4 come 100, etc. Espressi per convenienza coe numeri decimali, gli indirizzi IP sono realmente numeri binari; ad esempio l'indirizzo IP 209.191.4.240 è in formato ninario pari a 11010001.10111111.00000100.11110000. Si veda *bit*, *Indirizzo IP* e *Network Mask*.

bit

Forma contratta per "binary digit". Un bit è un numero con due soli possibili valori: 0 o 1. Si veda *binario*.

bps

bit al secondo (bits per second)

bridging

Il bridging è la tecnica per trasferire i dati dalla propria rete a quella dell'ISP e viceversa, utilizzando indirizzi hardware del dispositivo preposto alla funzione. La tecnica di Bridging è contrapposta a quella di routing, che può essere considerata più "intelligente" in quanto utilizza gli indirizzi di rete per ottimizzare il trasferimento dei dati. Il Router può effettuae sia routing che bridging. Tipicamente, quando entrambe le funzioni sono attive, il dispositivo utilizza la funzione di routing per i dati IP e la funzione di bridging per tutti gli altri tipi di dati. Si veda *routing*.

Broadband

E' una tecnologia di telecomunicazione che può inviare differenti tipi di dati sullo stesso 'media'. DSL è una tecnologia broadband.

Broadcast

Funzione che permette di inviare dati a tutti i computer sulla rete.

DHCP

Dynamic Host Configuration Protocol
Il DHCP automatizza l'assegnazione e la gestione degli indirizzi. Quando un computer si collega alla LAN, il DHCP gli assegna un indirizzo IP da un gruppo di indirizzi disponibili. Dopo un periodo di tempo predefinito, il DHCP ritorna l'indirizzo al gruppo di indirizzi disponibili.

DHCP relay

Dynamic Host Configuration Protocol relay
Un relè DHCP è un computer il cui compito è quello di reindirizzare i dati DHCP tra i computer che richiedono gli indirizzi P ed il server DHCP che li assegna. Ciascuna interfaccia del Router può essere configurata come un relè DHCP. Si veda *DHCP*.

DHCP server

Dynamic Host Configuration Protocol server
Un server DHCP è un computer che gestisce l'assegnazione degli indirizzi IP ai computer connessi sulla LAN. Si veda *DHCP*.

Digitale

Dati caratterizzati da un segnale discreto, le cui informazioni sono espresse come numeri binari (0 e 1). I dati in DSL sono registrati mediante segnali digitali. Si veda *analogico*.

DNS

Domain Name System
Il DNS realizza la mappatura dei nomi a dominio e dei relativi indirizzi IP Le informazioni DNS sono distribuite in forma gerarchica attraverso Internet, mediante computer denominati Server DNS. Ad esempio, *www.yahoo.com* è il nome a dominio associato all'indirizzo IP 216.115.108.243. Quando si avvia la connessione ad un sito WEB, un server DNS cerca il nome a dominio richiesto e ritorna il corrispondente indirizzo IP. Se il server DNS non trova

l'indirizzo IP corrispondente, reinvia la ricerca ad ulteriori server DNS di livello più alto per determinare l'indirizzo IP associato. Si veda *Nome a dominio.*

Domain name (nome a dominio)

Il Domain Name (nome del dominio) si usa per identificare in modo più semplice l'indirizzo IP ad esso associato. Il Domain Name deve essere unico; la loro assegnazione è controllata dalla Internet Corporation for Assigned Names and Numbers (ICANN). I Domain name sono gli elementi chiave per gli URL, ossia gli indirizzi che identificano un file specifico su un sito web. Si veda *DNS*.

Download

Operazione di trasferimento dei dati nella direzione di "downstream", ossia da Internet verso l'utente.

DSL

Digital Subscriber Line
Tecnologia che permette di far viaggiare dati digitali e voce analogica sulla stessa linea telefonica.

Encryption keys (chiavi di cifratura)

Si veda *Chiavi di rete*

Ethernet

La più comune tecnologia per la realizzazione di reti di computer, mediante l'utilizzo di cavi a coppie twistate. La velocità dei dati su reti Ethernet sono 10 Mbps e 100 Mbps. Si veda anche *10BASE-T*, *100BASE-T*, *coppia twistata*.

FTP

File Transfer Protocol
Programma utilizzato per trasferire file tra computer connessiad Internet. L'utilizzo più comune è quello di trasferire nuovi file o aggiornare quelli esistenti trasferendoli dal computer locale ad un web server e di scaricare file da un web server al proprio computer.

Gbps

Abbreviazione di Gigabits per second, ossia di un miliardi di bit per secondo. Le velocità in rete Internet sono spesso espresse in Gbps.

Host

Un dispositivo (tipicamente un computer) connesso alla rete.

HTTP

Hyper-Text Transfer Protocol
HTTP è il protocollo principale per trasferire i dati da siti Web allo scopo di farli visualizzare dal browser. Si veda *browser web*, *sito web*.

Hub

Un hub è un punto di convergenza dove i dati arrivano da uno o più direzioni e sono reinviati in una o più direzioni. E' utilizzato per collegare un bridge/router Ethernet ad un gruppo di PC su rete LAN e permette la comunicazione tra i dispositivi di rete.

ICMP

Internet Control Message Protocol
Protocollo Internet utilizzato per tracciare su report gli errori ed informazioni relative alla rete. Il comando ping usa il protocollo ICMP.

IEEE

Abbreviazione di "Institute of Electrical and Electronics Engineers" è una società di tecnici professionisti che promuove lo sviluppo di standard applicabili a livello nazionale ed internazionale.

Internet

Rete mondiale per l'interconnesione di reti per le comunicazioni private e commerciali.

Intranet

Rete ad uso privato che opera come una parte di Internet (gli utenti possono navigare mediante browser WEB), essendo acessibile agli utenti interni.

IP

Si veda *TCP/IP*.

IP Address (Indirizzo IP)

Indirizzo per Internet Protocol
L'indirizzo di un host (computer) in Internet, composto da quattro valori numerici, ciascuno nel range da 0 a 255, separati da pnti. Ad esempio 209.191.4.240. Un indirizzo IP consiste di un ID di rete (network ID) che identifica la rete in cui è connesso l'host ed un identificativo dell'host (Host ID) che identifica in modo univoco l'host all'interno della rete. Una Network Mask si utilizza per definire quale parte dell'indirizzo identifica la network ID e quale l' host ID. Poichè gli indirizzi IP sono difficili da ricordare, normalmente sono associati ad un nome a dominio che può essere utilizzato in alternativa. Si veda *Nome a dominio*, *Network Mask*.

ISP

Internet Service Provider
Una azienda che fornisce l'accesso alla rete Internet ai propri clienti, normalmente a pagamento.

LAN

Local Area Network
Una rete limitata ad una piccola area geografica, quale ad esempio una abitazione o ad un ufficio.

LED

Light Emitting Diode
Un dispositivo elettronico ad emissione di luce. Gli indicatori luminosi presenti sul frontale del Router sono LED.

MAC address

Media Access Control address
L'indirizzo hardware non modificabile assegnato ad un dispositivo dal costruttore. Gli indirizzi MAC sono espressi da 6 coppie di caratteri esadecimali, con ciascuna coppia di caratteri separati da ":". Per esempio: *NN:NN:NN:NN:NN:NN*.

Mask

Si veda *network mask*.

Mbps

Abbreviazione di Megabits per second, ossia di un milione di bit per secondo. Le velocità in rete sono spesso espresse in Mbps.

NAT

Network Address Translation
Un servizio disponibile su molti router che permette di traslare il proprio indirizzo IP pubblico sull' indirizzo IP privato di ciascun computer sulla rete LAN. Gli indirizzi di tipo privato sono utilizzati e noti solo al router ed ai dispositivi della propria rete LAN. Il mondo esterno (Internet) quando comunica con un computer della rete LAN vede esclusivamente l'indirizzo IP pubblico.

Network (rete)

Un gruppo di computer connessi tra loro, capaci di comunicare e condividere risorse quali software, file, etc. Una rete può essere piccola, come una LAN, o di grandi dimensioni, quali Internet.

Network mask

Una Network Mask è una sequenza di bit applicata ad un indirizzo IP per selezionare il Network ID, ignorando la parte relativa all' host ID. I bit impostati ad 1 indicano il "bit da utilizzare" mentre quelli impostati a 0 il "bit da ignorare". Per esempio, la Network Mask 255.255.255.0, quando applicata all'indirizzo IP 100.10.50.1, indica che il Network ID è 100.10.50 e l'host ID è 1. Si veda *binario*, *Indirizzo IP*, *subnet*.

NIC

Network Interface Card
Una scheda di rete installata nel computer che fornisce la connessione fisica ai cavi di rete. Per la rete Ethernet, l'interfaccia di rete utilizza tipicamente un connettore RJ-45. Si veda *Ethernet*, *RJ-45*.

Packet (pacchetto dati)

I dati trasmessi sulla rete sono raggruppati in strutture predefinite, chiamate pacchetti di dati. Ciascun pacchetto contiene un parte denominata payload (i dati) ed una parte di intestazione, in cui è registrato il mittente ed il destinatario.

Ping

Packet Internet (or Inter-Network) Groper
Un programma utilizzato per verificare se l'host associato all'indirizzo IP specificato è in linea. Può essere utilizzato per identificare un indirizzo IP per il nome a dominio specificato.

Porta

Un punto di accesso di un un dispositivo quale un computer o un router, attraverso cui può passare un flusso dati sia da che verso il dispositivo.

PPP

Point-to-Point Protocol
Protocollo per trasmissione dati di tipo seriale che è utilizzato per il trasporto di dati IP (e del protocollo IP) tra l'ISP ed il computer. L'interfaccia WAN del router utilizza due tipi di protocolli PPP, denominati rispettivamente PPPoA e PPPoE. Si veda *PPPoA*, *PPPoE*.

PPPoA

Point-to-Point Protocol over ATM
Uno dei due tipi di interfacce PPP che si possono definire per un Virtual Circuit (VC). La seconda è PPPoE. E' possibile definire solo una interfaccia PPPoA per ciascun VC.

PPPoE

Point-to-Point Protocol over Ethernet
Uno dei due tipi di interfacce PPP che si possono definire per un Virtual Circuit (VC). La seconda è PPPoA. E' possibile definire una o più interfaccia PPPoE per ciascun VC.

Protocollo

Il termine protocollo definisce un set di regole con cui gestire la trasmissione dei dati. Affinche una trasmissione dati possa operare correttamente, i dispositivi presenti ad entrambe le terminazioni del collegmento devono rispettare le regole imposte dal protocollo.

Remoto

Letteralmente, posto in una posizione fisica differente. Per esempio, un dipedente in viaggio che richiede l'accesso alla intranet aziendale viene definitoi come utente remoto.

RIP

Routing Information Protocol
Il protocollo originale per il routing TCP/IP. Esistono due versioni di RIP: versione I e versione II.

RJ-11

Registered Jack Standard-11
Il connettore standard utilizzato per collegare telefoni, fax, modem, etc. ad una presa telefonica. Tipicamente è un connettore a 6 pin, collegato mediante 4 fili.

RJ-45

Registered Jack Standard-45
Connettore 8 pin utilizzato per la trasmissione dei dati su linea telefonica. I cavi Ethernet normalmente utilizzano questo tipo di connettore.

Routing

Reindirizzamento dei dati tra la propria rete locale ed Internet mediante tecniche di instradamento ottimizzato, utilizzando le informazioni dell'indirizzo IP di destinazione e lo stato corrente della rete. Un dispositivo capace di effettuare la funzione di routing è denominato router.

SDNS

Secondary Domain Name System (server)
Identifica un Server DNS che si utilizza in sostituzione del Server priumario, quando questo non è disponibile. Si veda *DNS*.

Subnet

Una Subnet (o sottorete) è una porzione di una rete. La sottorete è identificata nella rete principale (più grande) mediante una Subnet Mask che permette di selezionare solo una parte dei computer connessi nella rete, escludendo tuti gli altri. I computer della sottorete rimangono fisicamente collegati ai restanti computer, ma li considerano come se fossero fisicamente collegati ad un'altra rete. Si veda *Network Mask.*

Subnet mask

Una maschera di bit che definisce una sottorete. Si veda *Network Mask*

TCP

Si veda *TCP/IP*.

TCP/IP

Transmission Control Protocol/Internet Protocol
Il protocollo di base utilizzato su Internet. Il protocollo TCP è utilizzato per dividere i dati in pacchetti idonei all'invio in rete e per riassemblare i dati quando raggiungono la destinazione. Il protocollo IP è utilizzato per il trasferimento dei dati dalla sorgente alla destinazione. Quando i protocolli TCP ed IP sono utilizzati in abbinamento a protocolli di livello superiore, quali HTTP, FTP, Telnet, etc., il protocollo TCP/IP diventa il riferimento per tali suite di protocolli.

Telnet

Applicativo di tipo console (visualizzazione testuale) utilizzato per accedere a computer remoti. Mentre l' HTTP (il protocollo WEB) e l' FTP permettono di effettuare download di file da computer remoti, Telnet permette di accedere al computer e di utilizzarlo da una postazione remota.

TFTP

Trivial File Transfer Protocol
Protocollo di trasferimento file, il TFTP è caratterizzato da un uso più semplice rispetto al protocollo FTP (File Transfer Protocol), ma non assicura le stesse capacità e sicurezza.

TKIP

Il protocollo TKIP (Temporal Key Integrity Protocol) fornisce la funzionalità WPA con cifratura dei dati. Tale protocollo assicura che venga generata una unica chiave master per ciascun pacchetto dati, supporta messaggi di integrità e regole di sequenzialità e supporta inoltre meccanismi di ricifratura.

Trigger

I Trigger si utilizzano per l'uso contemporaneo di più protocolli che creano sessioni separate. Alcune applicazioni, quali NetMeeting, aprono connessioni secondarie durante la normale operatività. Ad esempio, instaura una connessione con il server utilizzando una porta, ma i dati sono trasferiti con una connessione differente. Un trigger informa il dispositivo circa le connessioni secondarie che saranno aperte e le modalità per gestirle.

Una volta che si è predisposto un trigger, l'indirizzo IP nativo di ciascun pacchetto entrante è sostituito dall'indirizzo corretto dell'Host, così che il NAT può reindirizzare i pacchetti al corretto destinatario. Si può specificare se si vuole che venga sostituito l'indirizzo a, in caso, se debba essere sostituito sui soli pacchetti TCP, sui soli pacchetti UDP o su entrambi.

Twisted Pair (coppia twistata)

E' il normale doppino telefonico, utilizzato dalle compagnie dei telefoni. Contiene uno o più coppie di fili twistati (intrecciati) allo scopo di ridurne l'induttanza ed il rumore. Ciascuna linea telefonica ne usa una coppia. Nelle case si trovano spesso collegamenti realizzati con due coppie. Per le LAN Ethernet, si usano collegamenti di qualità superiore, denominati Categoria 3 (CAT 3), nel caso di reti 10BASE-T e di qualità ancora superiore, denominati Categoria 5 (CAT 5) per reti 100BASE-T. Si veda *10BASE-T*, *100BASE-T*, *Ethernet*.

Unnumbered Interface (interfacce non numerate)

Una interfaccia unnumbered è una interfaccia di tipo IP che non utilizza subnet locali. In sostituzione, tale interfaccia utilizza un Router-ID come indirizzo del sorgente e della destinazione dei pacchetti inviati da e verso il router. Al posto dell'indirizzo IP di una normale interfaccia, il Router-ID di una interfaccia unnumbered può essere assegnata con lo stesso indirizzo IP di un'altra interfaccia. Ad esempio, l'interfaccia WAN unnumbered del dispositivo usa lo stesso indirizzo IP della interfaccia LAN (10.0.0.2).

L'interfaccia unnumbered è temporanea – i protocolli PPP o DHCP assegneranno un indirizzo IP ‘reale’ automaticamente.

Upstream

Operazione di trasferimento dei dati dall'utente verso Internet.

VC

Virtual Circuit
Una connessione dal Router DSL al vostro ISP.

VCI

Virtual Circuit Identifier
Insieme al Virtual Path Identifier (VPI), il VCI identifica univocamente un VC. L' ISP comunicherà un VCI per ciascun VC fornito. Si veda *VC*.

VPI

Virtual Path Identifier
Insieme al Virtual Circuit Identifier (VCI), il VPI identifica univocamente un VC. L' ISP comunicherà un VPI per ciascun VC fornito. Si veda *VC*.

WAN

Wide Area Network
Qualsiasi rete estesa ad una vasta area geografica, quale una nazione o un continente. Rispetto al Router, la WAN fa riferimento ad Internet.

Web browser

Una applicazione che utilizza il protocollo HTTP (Hyper-Text Transfer Protocol) per scaricare informazioni da siti web (o per effettuare l'upload verso i siti web), visualizzando le pagine WEB contenenti testi, immagini, audio o video. Tutti i Web browser utilizzano il protocollo HTTP (Hyper-Text Transfer Protocol). I più diffusi Web browser sono Netscape Navigator e Microsoft Internet Explorer. Si veda *HTTP*, *sito Web*, *WWW*.

Web Page (pagina Web)

Un file di un web site tipicamente contenente testo, grafica e hyperlinks (collegamenti testuali) ad altre pagine dello stesso sito o di altri siti. Quando si accede ad un sito, normalmente la prima pagina visualizzata si definisce home page. Si veda *hyperlink*, *sito web*.

Web site (sito Web)

Un computer nella rete Internet che distribuisce informazioni ad utenti remoti (o prende informazioni da essi) attraverso browser Web. Un sito Web tipicamente consiste di pagine Web che contengono testi, grafica e hyperlink. Si veda *hyperlink*, *pagina web*.

WWW

World Wide Web
Anche definito come “*il WEB”*. Termine con cui si comprendono tutti i siti web distribuiti sull'intero globo e che possono essere visitati attraverso Internet.